

Volume Thirty-Five Number Two

DIGITAL EDITION Summer 2018

2600

The Hacker Quarterly



Payphones Plus



Portugal. Many say that the age of shoeshining is over. Many say the same thing about payphones. So why not combine the two as this entrepreneur in Lisbon is doing? It's one way to get a chair back into a phone booth.

Photo by Galia Kaplan



United States. We actually saw this very phone in our 2017 Hacker Calendar, but now it's apparently gotten the attention of the sun, which makes it so much more than a lowly payphone in Muir Woods National Monument, California.

Photo by Artem Skortsesskul

Booths With Beer



Canary Islands. We may need a new page for this theme. So many phones lately seem to have beverages attached. This one was found on the island of Tenerife. (San Miguel beer is from the Philippines, but has become very popular in this region.)

Photo by Kai Kramhöft



Japan. No confusion here. It's a Japanese phone by a Japanese train with a Japanese beer. Asahi is clearly the choice of the subway riding payphone user. Seen at the Higashi-Nakano station in Tokyo.

Photo by John Klacsmann

Got foreign payphone photos for us? Email them to payphones@2600.com. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (More photos on inside back cover)

PROCEDURES

Celebrate the Difference	4
A NOOb's Guide to the Dark Web	6
The IPv6 Delusion	8
TELECOM INFORMER	13
How to Be a Guitar Hero, IRL	15
Even Restaurants Need InfoSec	20
Serial Number Cracking For Fun and Profit	22
Automating a Police State	25
HACKER PERSPECTIVE	26
Brute Forcing a Car Door with Math	29
Hack(ed), the Earth	32
LETTERS	34
EFFECTING DIGITAL FREEDOM	46
A Hacker Adventure in Urban Exploration	47
Beyond the Scare-Mongering	50
CITIZEN ENGINEER	52
Re-Purposing Old Technology and Ideas for Fun and Emotional Profit	54
Hacking: Quick and Easy	56
Thoughts On Cryptocurrency	57
Fiction: Hacking the Naked Princess 0x15	58
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

Celebrate the Difference

"Crayons" by idreamlikecrazy is licensed under CC BY 2.0

We may not have ever lived through a more contentious time. There have certainly been all sorts of conflicts and differences of opinion over the years. But nothing like this, where we see on a daily basis two entirely separate worlds being portrayed, whether it be within government, the media, or our own homes. It's almost enough to make us want to stop paying attention altogether.

Debate is healthy. Having opposing views is what forces us to defend our own, and either learn how to bolster the arguments that make sense and discard the ones that don't, or become swayed by the points being made from the other side. But, in order to do this, we need to actually take the other side seriously. We need to respect them. We need to listen.

The hacker community has always been about differences. In the earlier days, these differences were mostly isolated to people who didn't fit in with the rest of society because of their interests in phones, computers, or technology in general. But it was still mostly a white male dominated thing, as was far too much of our culture. In later years, however, we've seen a natural progression and an openness that is welcoming to other backgrounds of all sorts. It fills us with pride to see the diversity represented at our HOPE conferences, especially because this is something that didn't have to be artificially induced. Don't get us wrong; we know we have a long way to go. But, in this time when so many doors are being slammed shut, it's heartening to see our community listening, learning, and holding our door open.

This is no easy task, especially these days. The instinct to shut out the people we see as responsible for all of the negativity is quite powerful. But that is precisely when being reflective is what is needed most. Are they indeed the ones responsible? What do we gain by no longer listening or even acknowledging?

In these pages, at our conferences, and on our radio broadcasts, we try to be as open as possible to differing viewpoints and perspectives. It would be boring if we stuck to one agenda and didn't even entertain the notion that there could possibly be another way - or that we might be completely wrong. Again, doing this allows us to strengthen our own arguments and reexamine their effectiveness. This better prepares us to defend the positions we hold. Always being open to changing those positions based on the arguments we're confronted with is how dialogue moves forward. And this is what much of mainstream society seems to have lost in recent years.

Of course, it's really hard to do any of this if basic components of facts, statistics, history, science, etc., are ignored or distorted. This is a side effect of believing one's side is *always* right. Even when the facts make it painfully obvious how wrong we are, we twist those facts or try to discredit them entirely in order to preserve our conclusions. This starts the ball rolling. Your opponent no longer takes you seriously and eventually stops paying attention to anything you say because it's based on false premises. You retort with a distraction or an accusation of some sort that diverts the conversation away from the actual topic. Nothing is accomplished, other than to firmly establish barriers between the two sides with no opportunity to learn or change one another's minds. Neither side listens to the other and everyone lives in a stalemate.

So much of this can be avoided with a few simple steps. First, we have to all accept that not every argument is deserving of equal respect. Sure, there are people who don't believe in gravity or who think the earth is flat. It's an interesting aside, but nothing is gained by propelling these positions into a corresponding seat at the table when it comes to discussing science. To do so simply holds

everyone back from any kind of advancement. People who can't accept certain obvious and easily provable facts will always be around. Once their premise has been disproved, it's time for the rest of us to move on. But that can't happen if otherwise reasonable people somehow feel an allegiance to these misled individuals - *or* if the rest of us overgeneralize and try to label everyone who doesn't buy into all of our premises as equally backwards and ignorant. That is how you inadvertently build strong alliances based on facts that don't add up. It's no longer about the facts, but about the resistance to being told how you must think and what you must support. If nothing else, *that* is the common ground that unites us: nobody likes to be told what to do.

This is where those of us who oppose much of what's going on today could stand to do a better job. Rather than dismiss people who have reached different conclusions entirely, why not try to find that common ground? Certainly there will be cases where this isn't possible and where you will literally come up against an adversary that wishes for your annihilation. But, at least for now, that's still the exception rather than the rule. Most times you can listen, you can go over facts, and you can either sway an opinion or not. It's the dialogue itself that's the accomplishment, providing we listen, respect one another, and don't hold back with our own arguments and views. Just establishing that link is often enough to change someone's perspective significantly.

Many of us have had to engage in such exercises within our own families. Add in the inevitable emotions and history, and this kind of thing can be either a curse or an opportunity. But the only real failure is in not trying to communicate at all.

That's the message we should all try and remember as we keep moving down this road. We are all different - and that is a really good thing. We would learn very little from other people if they were just like us. Inevitably, there will be things we find objectionable, even abhorrent, about virtually any other person. That doesn't mean we can't still reach them and possibly resolve these issues. And if we truly can't, knowing that we made the effort really matters. It's when we start dismissing people out of hand for where they're from, what they support, or who they're allied with that we start to really add up the missed


opportunities.

None of this should imply that we need to back down in any way from the strength of our convictions. Done correctly, this will only make them stronger. It's when we choose to eliminate challenges and only converse with like-minded people that we really lose. We not only lose these opportunities, but we lose sight of what is real. And that's how unexpected things wind up happening, leaving us to wonder why we didn't see them coming. It's because we weren't engaged in the conversation. It's because we weren't paying attention to what was going on all around us. It's because we chose to feel safe in our own insulated world.

Social media has made it so much easier to find those people that we're similar to. While that initially seemed like a good thing, it may well turn out to be an albatross. By only exposing ourselves to a particular point of view or philosophy, it's that much easier to be outraged when something opposing that comes along. These "others" then become the enemy and, more often than not, we isolate ourselves from them. Demonization and lack of communication are the ingredients that drive any conflict, only now this seems to be our default manner of handling relationships. We even begin to apply a purity formula to those around us, further isolating ourselves from those who disagree on even a single issue. Clearly, this is not healthy.

In the hacker world, we have always embraced dissent of one sort or another. We will thrive as long as we continue to do this. We must also embrace debate and disagreement in our midst, since that is how we learn and strengthen our own arguments. It's great to have our "safe spaces" to regenerate in. But spending too much time there only makes us weaker and less able to see what's actually going on.

What we ultimately want to see are individuals unafraid of standing up for what they believe in, even if they're the only ones in a crowd, and even if that crowd is composed of their own friends. We want to see these individuals supported, even celebrated, because of the strength they're showing. It's easy to fit into a crowd. But encouraging individual thought above all else is what this community should always be about.



A NOOb's Guide to the Dark Web

"Stormy Paris" by theBlastart is licensed under CC BY-NC-ND 3.0

by **Kim Crawley**
Twitter: @kim_crawley

Before I get a chance to read it, I already know that this issue of *2600* is full of esoteric hacks and little known vulnerabilities. That's great; that's the sort of material that *2600* readers can always depend on. It's why *2600* is as important now as it was back in 1984, the year both myself and this fine publication were born.

But for every handful of *2600* readers who know how to print "Hello world" to the LCD displays of IoT refrigerators from their phone without having to look up how to do it, there's got to be a reader who hears "Dark Web this," "Dark Web that," and doesn't know how to access it. Everyone's a n00b at some point in their lives. For you dear n00bs, this article is for you.

What is the Dark Web?

The Dark Web is the corner of the World Wide Web that's only accessible with anonymizing technologies such as special combinations of proxy servers and encryption. The Dark Web consists of web pages that you usually can't load in your web browser without a Tor, Freenet, or I2P client of some kind. It's often confused with the Deep Web. Don't be fooled - the Deep Web is the part of the World Wide Web that can't be easily searched with Google or Duck Duck Go because the web pages are so old and/or they don't have many links that webcrawler bots can use to find them. Illegal drug marketplaces are part of the Dark Web. The Spice Girls fan website I made on Angelfire in 1996 that I hope no one finds is part of the Deep Web. It's an important distinction. Sometimes the Dark Web is considered to be a part of the Deep Web because any web page that can't be web searched in a more conventional way is Deep. But keep in mind

that most of the Deep Web isn't part of the Dark Web. Whew!

Understanding the culture of the Dark Web requires the sort of nuance that the mainstream media typically lacks. Yes, people often use the Dark Web because they're engaging in illegal activity and they don't want to be traced by law enforcement. The Silk Road and several other illegal drug marketplaces have come and gone from the Dark Web over the years. Script kiddies often buy malware scripts on the Dark Web so they can engage in various cyber attacks without having to code. Someone who sells child pornography will use the Dark Web for distribution and cryptocurrency as payment. Think about that for a second. Both the Dark Web and cryptocurrency enable the evil exploitation of children. But why do laypeople hear "Bitcoin" and associate it with getting rich quick, but they hear "Dark Web" and think about bad people doing bad things? Both the Dark Web and cryptocurrency are means for bad people to do bad things. But so are BIC lighters. Fire is a deadly weapon or a lifesaver from hypothermia depending on how someone uses it.

Sometimes people use the Tor network and the Dark Web because they're journalists who need to share information about the dangerous politicians who would have them arrested. Edward Snowden's NSA leaks and Vault 7 on WikiLeaks should have taught everyone that the American government and other powerful entities will exploit the Internet in order to violate the privacy of innocent people. No national governments or large corporations are without some degree of corruption and evil. Now law enforcement may be able to track the movement of your IoT car and look at the contents of your IoT fridge. They might use Google Home or Amazon Echo or your child's nifty new toy to watch her while you read her a bedtime story.

Whether or not something is legal doesn't determine whether or not something is moral. But cracking down on child pornographers is a very good thing to do. I just hope law enforcement uses the Dark Web to investigate pedophiles without violating the rights of people who have no reason to be suspects. That won't happen, of course.

What's Tor?

Tor is The Onion Router network. Tor is one of the technological backbones of the Dark Web. You will need to install a Tor client in order to access it. Freenet and I2P are technologically similar but different routing technologies that are used in the Dark Web. But Tor is the most widely implemented and using Tor gives you access to more of the Dark Web than any other system. Interestingly enough though, only about three percent of Tor network traffic is used for the Dark Web! For the sake of simplicity, this guide focuses on Tor, but you should be aware that there are alternatives.

Development of Tor started in 1995. Visit <https://www.onion-router.net/History.html> for further details. The Tor design document (<https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf>) was published in 2004. Only in the past decade or so have easy-to-use stable Tor clients been available that make using Tor really simple for people who aren't computer networking geeks.

Here's how Tor works in a nutshell. Tor protects against traffic analysis Internet surveillance. Tor usually makes it very difficult for third parties to figure out which Onion-routed Internet servers have been sending data to your client machine, whether it's a PC, smartphone, touchscreen ARM system embedded in a women's clothing store mannequin, or whatever. It's called The Onion Router because your Internet traffic within that network is routed between metaphorical layers of proxy servers, like an onion.

This is how Tor Project describes its name: *"Because Tor is the onion routing network. When we were starting the new next-generation design and implementation of onion routing in 2001-2002, we would tell people we were working on onion routing, and they would say 'Neat. Which one?' Even if onion routing has become a standard household term, Tor was born out of the actual onion routing project*

run by the Naval Research Lab. (It's also got a fine translation from German and Turkish.)

Note: even though it originally came from an acronym, Tor is not spelled 'TOR.' Only the first letter is capitalized. In fact, we can usually spot people who haven't read any of our website (and have instead learned everything they know about Tor from news articles) by the fact that they spell it wrong."

Web URLs on the Tor network use the ".onion" top level domain.

This is what happens when a client machine successfully uses the Tor network. The user's Tor client acquires a list of available Tor nodes from a directory server. When the user tries to access a web page from a Tor URL, a random path will be taken through available Tor nodes and proxy servers. The traffic's entrance to the Tor network goes through an entry node, the traffic is routed through a few random proxy servers, then the traffic is routed to the desired Tor network Internet resource, such as a web server, through an exit node. Traffic to the entry node and traffic that leaves the exit node is in plaintext, whereas all of the traffic inside the Tor network is encrypted. Traffic from the Tor-delivered website back to the client machine, such as HTML web pages and web page embedded media, gets sent back through the same path in the opposite direction. Keep in mind that Tor isn't just used for the web, but also for many other Internet services such as IRC chat or email. But Tor web browsers are the most frequently used Tor clients.

People volunteer to operate Tor entry and exit nodes and proxy servers. The Tor network is physically manifested worldwide just as all of the other parts of the Internet are which aren't a part of the Tor network.

Here's the best way to use Tor to access Dark Web sites:

The Tor project recommends that you use the open source Tor browser in order to access Tor-protected websites. There are Tor browsers for Windows, macOS, Linux, and Android which can be downloaded from <https://www.torproject.org/download/download.html.en>. Alternatively, you can compile Tor browser from source code that can be found through the same web page.

You can use the Tor browser to access ordinary websites, not only ".onion" websites. Feel free to test <https://www.2600.com/> in your Tor browser. It should work just fine.

Keep in mind that any web page you access through the Tor browser will probably take longer to download than when you visit web pages outside of the Tor network. Routing web traffic through proxy servers slows it down. That's why I don't use the Tor browser to access ordinary websites, but your mileage may vary.

When you launch the Tor browser, you need to activate a connection to the Tor network through the browser's GUI. The Tor browser's GUI will also indicate whether or not you're securely connected to the Tor network at any given time. You can only access ".onion" websites while you have an active connection to the Tor network.

The Tor network recommends that you don't install web browser plugins in your Tor browser. If you like to use specific web browser plugins for any particular reason, you should be doing so while using a mainstream web browser such as Chrome, Firefox, or Safari. Some plugins such as Adobe Flash can reveal your IP address to third parties and the Tor project doesn't want to take that risk.

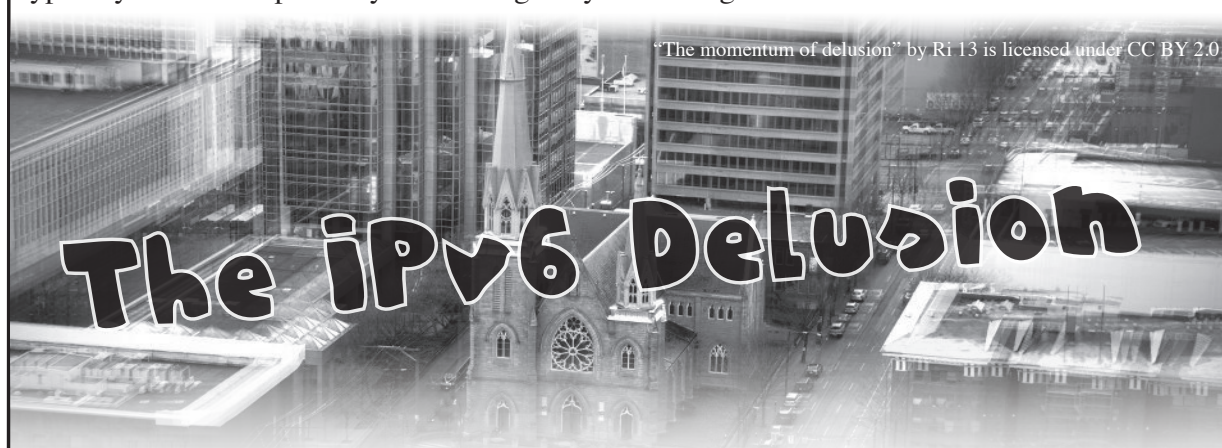
BitTorrent clients will usually ignore proxy server settings. Also, torrenting generates a lot more traffic than most other Internet services typically do. It's probably technologically

possible to develop a BitTorrent web application if it hasn't been done already. If they exist, you shouldn't use them with your Tor browser. For security and practicality reasons, BitTorrent doesn't play nicely with Tor. Please don't do it!

The Tor project recommends that you always use HTTPS (via port 443) instead of HTTP (via port 80). HTTPS Everywhere is built into the Tor browser for that purpose. Using HTTPS means that your web traffic outside of the Tor network will also be encrypted.

Google and Duck Duck Go won't work very well when you want to search for a Tor webpage. Also, ".onion" URLs tend to change a lot more frequently than typical web URLs do. If you want to do a web search of Tor-protected websites, I recommend trying Ahmia at <https://ahmia.fi/> or Torch Tor Search at <http://www.torchtorsearch.com/>.

There are lots and lots of Dark Web and Deep Web sites that don't exist to sell cocaine or malware or kiddie porn or firearms. Using Tor is perfectly legal in most countries. It's only the contents and activities on some Dark Web sites that are generally illegal. Happy hunting!



by David Crowe
David.Crowe@cnp-wireless.com

The Short Version

Let me keep it short. IPv6 is intended to vastly increase the number of Internet addresses. It will do this when the entire Internet has converted and when there are no IPv4-only clients or servers left. This will never happen, therefore IPv6 is a massive failure.

This is way too short to qualify for an

article in the esteemed 2600 journal.

The Topical Version

Let me be more topical. IPv6 is to the Internet what Donald Trump is to presidenting. It is true that Donald Trump is a living human being (at time of writing, anyway) and he meets most definitions of a sentient human, just as IPv6 is an existing protocol that even has its own IETF RFCs. And Donald Trump does do presidenting, at least when he's not golfing or watching fake news. But the real

work of managing the U.S. government is done by thousands of workers droning away in their Washington offices (at least when the government isn't shut down), planning where to invade next (sorry Michael Moore). Just like IPv6 does occasionally send packets through the Internet even though the vast bulk of message transmissions use IPv4.

IPv6 Gets Older, But Doesn't Reach Adulthood

Happy adulthood, IPv6, you are now 21, an adult no matter where you go in the world, although maybe you still can't rent a car in all locations. But what have you accomplished so far, you wastrel? So much has been written about your promise, but you just sit around the bar, complaining about your older sister while she is busy carrying packets hither and yon from one end of the Internet to the other. She has time neither to drink nor to complain.

IPv4 was designed to support four billion addresses. Perhaps it is better to say that IPv4 was designed with a 32-bit address, which supports two to the power of 32 different addresses, which is just over four billion - 4,294,967,296 if you like to be precise.

But hold on a minute! Surely there are more than four billion Internet accessing devices in the world? Every cell phone, every smart thermostat, every aging laptop, every server. Why haven't we run out already?

Well, it is because IPv4 is so NAT-ily dressed. She is a mistress of disguise with a different boyfriend in every port. Yes, the ports have saved us. It is a lucky coincidence that both TCP and UDP were designed with 16-bit ports, a concept slavishly copied by the other transport protocols that followed. This means that you don't need a real, i.e., public, IPv4 address until you actually want to bravely wander through the Internet swamp in your knee-high rubber boots. Your NAT (Network Address Translation device, such as a firewall or router) tags every outgoing packet with one of the real IP addresses associated with your network, and a port number currently unused by that IP address. When a response is received by your NAT, the combination of public IPv4 address and port number can identify the internal IPv4 address. When you're not transmitting, the ports can be recycled for others on your network.

Just the Facts, Ma'am

What this really means is that the IPv4 address is not really 32 bits in length, but 48. That there aren't just four billion addresses, but 281,474,976,710,656 - 281 trillion plus change. Now, not all of these can be used, because servers cannot play this NAT-ty trick in the same way, and an individual Internet device may require multiple ports because of multiple simultaneous TCP connections, for example, but even if only one percent of these addresses could be used, that still would support two or three trillion devices.

This doesn't come without a price. When NATs were first implemented, they broke a lot of software. But when push came to shove, the NATs pushed harder, and the broken software was either fixed or abandoned. There are other more subtle problems. Since the NAT doesn't know if a session is alive, it will either consume ports when it doesn't need to or timeout a transaction and recycle the port when a transaction is still outstanding. Some software sends "keep alive" messages to avoid losing the port to the outside world, and this wastes battery life on mobile devices. These problems have somewhat been ameliorated with new protocols and definitely don't qualify as a show stopper. Nothing can stop the IPv4 maven, mavening her way around the Internet with a million packets in each hand!

Acne and Cancer

If IPv4's problems are acne, IPv6's are terminal cancer.

All of its problems derive from arrogance, the arrogance that IPv6 was going to be a completely separate network, with no backwards compatibility with IPv4. The IPv6 network would grow and grow and IPv4 would wither away. How'd that work out for you IPv6, you lousy barfly?

Not well. Imagine you were the first IPv6-capable computer. Who could you talk to? You're on a barstool in a bar that hasn't hired its first bartender. Hard to get a drink, isn't it? So, after feeling awesome for a while because you're in a fancy new bar, you decide that loneliness sucks and you stagger back to the IPv4 bar. Well, walk actually, because even your plan of getting horribly drunk hasn't worked out. Yes, the IPv4 bar could use a new coat of paint, but hell, there's a party going

on! The booze is flowing like IPv4 packets at busy hour!

Stick Your Dual Stack Where the Sun Don't Shine

To avoid loneliness and depression, IPv6 devices still have to support IPv4, known as dual-stack. But if you can talk to the whole world with your IPv4 stack, what the heck do you need IPv6 for?

And even though a lot of devices now have dual stack, and therefore have an IPv6 address, how many IPv4 addresses has this saved? Right, zero. So the fundamental benefit of IPv6 won't be realized until... never.

Even if IPv6 is used (and it is, bizarrely enough), it doesn't save addresses.

It gets worse. Because the whole network needs to be duplicated, there was no thought about interworking between IPv6 and IPv4. So, ad-hoc methods were developed instead of having a standard prefix to indicate an embedded IPv4 address (e.g. 196 zeroes followed by the embedded IPv4 address).

And worse. You need a new DNS infrastructure, and this introduces nasty problems. Let's say that a heavy DNS user, such as a browser, sends out all queries to both the IPv6 (AAAA server) and the IPv4 (AAA). In many cases, the IPv6 query will not result in a response and, when it does, it will usually be slower. There is no benefit in a browser waiting for IPv6 when IPv4 has already responded. So what's the benefit of querying IPv6 at all? The impact of all these delays would destroy browser performance, so no matter how much the nerdy browser coders are excited by IPv6, they love their performance more.

IPv6 missionaries (and there are a few, hermits really, limited to the tiny world of the IPv6 Internet) claim that one advantage is that IPv6 will get rid of the need for NAT, and now you could have a unique and permanent IP address.

Well, except that now all Internet software is NAT-aware. And, another problem is that an IP address is not really an address. Well, it is an address, but an address of an interface card, and not of a device, let alone a user.

You can figure this out for yourself if you go into the settings on your phone, tablet, or computer. Every interface will have its own MAC address (which identifies the physical

hardware for ever and ever, amen) and, if the interface is connected, it will have its own IP address. And each network will have a different set of IP addresses. If you overstay your welcome at one coffee shop and go to another, you'll get a different IP address. And this will be just as true for IPv6 as for IPv4. The only exception is that if you get a private IP address from a network, it could coincidentally be the same as an address from another network, but through the magic of NAT is actually different.

So, nobody will walk around with their IPv6 address proudly scribbled on a piece of paper in their pocket. Which is another problem. You can remember IPv4 addresses, because they are usually represented as a quadruplet of decimal numbers, each being from 0 to 255. Something like 192.168.1.1 (a common private address) or 127.0.0.1 (which refers to the host computer). But you can't remember IPv6 addresses because they're too damn long.

Liars Figure and Figures Lie

Some of your readers may Google IPv6 and tell me that I'm BS'ing because Google (as of January 2018) is claiming that about 22 percent of their traffic is coming in over IPv6 (<https://www.google.com/intl/en/ipv6/statistics.html>). And further, that this is a huge rise from only about one percent in 2013. And these skeptics can find even more optimism at <http://www.worldipv6launch.org/info-graphic/>, which proudly proclaims, "IPv6 to the rescue" (they also say that, "without [IPv6] there just aren't enough Internet addresses to go around," which is a bald-faced lie, but missionaries were allowed to lie if necessary to save your soul). They show the Google graph and lie again: "If the trend continues, IPv6 will be the dominant protocol within about four years" (three years, since they haven't updated the graph in over a year, something that is common with IPv6 missionary websites that seem to come and go). This is a lie because the graph is just Google data, and few companies are as gung-ho on IPv6 as them and, in many non-English speaking countries, Google is not the dominant search engine. (Anybody heard of China? Russia?)

The truth is out there if you look hard enough. AMS-IX, the Amsterdam Internet Exchange, is a small Internet connectivity hub. Small in that traffic has gone from 1,200 terabytes a month at the end of 2001 to 1,200,000 terabytes by the end of 2017. Actually, I lie, they are the second largest Internet exchange in the world.

And, how much of their traffic is IPv6, you want to know? You really want to know, don't you? Ahem, I'll give you a hint. It's not looking good... for IPv6. Unfortunately, they only give the data for the last year, but this should be the best year ever for IPv6 and, well, this is a bit embarrassing. IPv6 traffic is almost invisible at under two percent, with IPv4 responsible for the other 98 percent (<https://ams-ix.net/technical/statistics/sflow-stats/ether-type>).

Maybe I'm just cherry picking and I've found an Internet exchange with an abnormally low rate of IPv6 traffic. Which is not likely, since it is the second largest in the world, and obviously supports IPv6 quite nicely. In fact, the nice folks at World IPv6 Launch emphasize the relevance of this data by highlighting a graph of AMS-IX IPv6 traffic on their site, using it as an example of growing traffic (<https://ams-ix.net/technical/statistics/sflow-stats/ipv6-traffic>).

Dosh garn it, the graph does look impressive! (because IPv4 traffic is not on the graph - good trick guys) with traffic rising from about 50 Gbps (billion bits per second) in April 2017 to about 70 Gbps in January of 2018. So the total monthly IPv6 traffic is about 70Gb/sec times 2,629,800 seconds/month (approximately, because not every month is the same length) divided by eight to convert from bits to bytes, and dividing by 1,000 to convert from giga to tera. In other words, monthly IPv6 traffic is the unfathomably huge number of 23,011 terabytes. Which sounds impressive, until you realize that it is less than two percent of their total 1,200,000 terabytes (as shown by their other graphs).

This company unfortunately doesn't keep historical statistics of IPv4 versus IPv6, but I was able to find two snapshots on the Internet Archive, one from October 2013 and one from October 2015. These show that IPv6 traffic has risen by a factor of more than four since

2013. Wow! From a massive 0.4 percent to an amazing, awesome, incredible, but still rather minuscule, 1.8 percent in January, 2018. Um, maybe not so great.

If we extrapolate, which is always dangerous, it will take 298 years for IPv6 to become 100 percent of Internet traffic, at least on this one Internet exchange (the largest does not provide any IPv6 statistics). That's the year 2316, by which time the oceans will be boiling if we extrapolate current climate statistics, so maybe we'll have worse things to worry about.

So What?

Psychologically, the IPv6 phenomenon is very interesting. When geeks latch onto a new technology, they won't let go until the flesh has rotted off the corpse, and it is just a dry skeleton. IPv6 still has a pulse, a faint pulse, so they are happy to tell you it ain't dead yet. For some cultists, you would probably have to burn all copies of all the IPv6 RFCs before they would believe the obvious truth. And everyone who is not a geek trusts nerds on important matters like this, because they assume only they are smart enough to figure it out. "Obviously," they think, "IPv6 must be just around the corner or else the geeks wouldn't keep bowing down and burning incense." But something is burning - it's the companies spending money on IPv6 (although, if you need dual stack to get a contract, I guess it's worth it).

So why do I care? I care because the Internet needs a new protocol for addressing, and it won't get one until IPv6 is abandoned. IPv7, which is the obvious new name, will obviously also have a larger address than IPv4 (although maybe 128 bits is excessive), but will be backwards and forwards compatible with IPv4. It will start as a parasite and gradually suck the life out of IPv4 until it is bigger than its host. And, as it grows, the need for IPv4 addresses will fall, so nobody will care if, 100 years from now, only the 2600.com server is still running with IPv4. Everyone can still talk to everyone. And when the final IPv4 server is powered down for the last time, the eulogies for IPv4 will be so moving. She did, after all, serve so many, so well, for so long.

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.)



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

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



TELECOM INFORMER

by The Prophet



Hello, and greetings from the Central Office! The Great Toilet Debacle of 2018 continues pungently apace. As you might recall from my last column, the giant cottonwood trees on our property line have grown their root system across the parking lot which wreaked all sorts of havoc on the sewer line. It wasn't a simple call to a plumbing company. We need an entirely new sewer line, haven't had working toilets in months, and I'm getting tired of visiting what we've named "Bella," the port-a-potty in our parking lot.

I thought I'd be able to fix more problems when I went into management. To some degree, I have (accelerating fiber-to-the-node deployment has both penciled out from a business perspective and provided better service to customers), but Central Office managers operate under considerable constraints. Even if I have a surplus, I can't move money around between different budgets, particularly between regulated and unregulated services (that's a *big* no-no). Flushing toilets in the Central Office are part of the company facilities budget, which is different from the collocated facilities budget, which is different from the various network, staffing, and vendor budgets. Since I already spent most of this year's facilities budget on keeping the roof from leaking this winter, I can't fix the sewer line unless I can convince the bean counters in Denver to let me do it. In all honesty, this probably wouldn't be a problem, but there are only two of them, and they work every request in a queue. The company does prioritize requests, but these are based on customer impact and protection of company assets. And although the company claims employees are its biggest asset, providing a port-a-potty is sufficient "protection" to keep my request at a lower priority in the queue. I'm guessing I'll finally get approval a week or two before the fiscal year resets on June 30th and I could have just taken care of the problem without any extra approvals. And yes, I know there's a backhoe in the yard, and we have most of the supplies to fix this on our own, but we're a union workforce and nobody's union contract involves fixing sewer lines. Don't even get me started on how much trouble I'd get in if I tried to work around *that*.

But I digress. It's merger time again and that

means more visitors to the Central Office. Under the Telecommunications Act of 1996, we were legally required to lease space to other phone companies and provide them the ability to interconnect with our networks. The original idea was to allow competitive local exchange carriers (CLECs) access to our networks, both on a resale basis (wherein we'd operate the services but they'd bill for them - sort of a "white label" or "private label" service) and on a facilities-based interconnection basis. In the 1990s and early 2000s, the most popular facilities-based interconnection was competitive Internet service providers offering ADSL services. They'd pay to lease "last mile" copper from us, and we'd terminate it at their DSLAM collocated in our Central Office. This business model began to go by the wayside in the late 2000s, as ADSL ran up against the technological limitations of an old copper network. We made the decision to invest in fiber to the node, and in an incredible gift from both the FCC and the state utilities commission, we weren't required to support "line sharing" ADSL on lines where we made this investment. This runs at speeds that are competitive with cable, but as we have slowly bled off the number of circuits where it's even possible to compete with line sharing ADSL, and as ADSL technology has failed to advance when running over long distances, an increasing number of competitors have merged, gone out of business, or begun reselling our services. They cut their customers over, then clean out their colo cage. Most of the cages are empty these days.

Even though far fewer competitive telephone companies collocate in our facilities than did even ten years ago, all of the major wireless carriers have a physical presence in my Central Office. They use this presence to connect their towers with their own networks; we operate the facilities in between the Central Office and their tower, but they pick up the traffic at our Central Office and drop it off onto their network. None of this stuff is configured as conventional voice trunks and none of it runs over the public Internet or frame relay networks. Instead, they have provisioned varying speeds of very expensive dedicated data circuits, sold at regulated prices. That's great for us here in the Central Office, because as wireless users' data

demands increase, the size of these circuits just keeps getting bigger - and the more we can charge for them. In fact, one of the big reasons why mobile data service is so expensive is paying for local telephone company charges to get that traffic from local networks out onto the public Internet.

Given the high costs involved, one of the first things mobile phone companies look to do when merging is to downsize duplicate infrastructure. Two major wireless carriers (let's call them "Yellow" and "Purple") have been engaged in an on-again, off-again attempt to merge for over a year. Well, it's on again, and network planning teams are making almost nonstop tours to my Central Office trying to figure out what to do. And they have a big, ugly integration problem on their hands.

One of the two companies, "Yellow," has been through a merger before. It was a tough, gnarly, drawn-out merger. The networks never really merged. There were entirely different technologies involved in almost every respect, and given that the acquired company had out-of-date technology, the eventual plan they arrived at was to leave most of the legacy infrastructure in place and sunset it (which finally happened late in 2013). However, the company made a real effort to consolidate duplicate infrastructure in the meantime. This was a lot easier said than done, though. The acquired company was technically using taxi dispatch frequencies which meant that some telecommunications services they used were tariffed differently and couldn't be intermingled across services. Of course, this was great for us, because it meant that "yellow" had to pay us twice for services they could have otherwise consolidated. There is an entire unit at our company dedicated to ensuring that tariffed services are correctly charged, at least when the billing isn't in our favor!

This time around, it's far more complicated, because even if the merged company chose to build a 5G network and sunset the rest, it's going to be a long time before that can really happen and it'll be a Herculean engineering effort to accomplish. It's also a complicated business proposition. The "Yellow" company, having fallen on hard financial times, spun off its network some time ago as a separate operating company (a few years after it sold off most of its towers to Crown Castle and American Tower). The status of this operating company and its future within the larger organization is very much in question at present, which is one very awkward wrinkle. No technician wants to work on legacy technology with a fixed sunset date and no job at the other end of it!

Another wrinkle is that the "Purple" company has historically had a very different approach to both technology and network design. This isn't a

network that can easily be glued together; one 4G network was built on top of an existing CDMA network and the other 4G network was built on top of an existing GSM network. What's more, the CDMA network on the "Yellow" side is still in use for carrying voice calls; "Yellow" never successfully implemented VoLTE. While this isn't particularly meaningful to us here in the Central Office, it does mean that it's a harder network to integrate. It won't be possible to just flip a switch and integrate this network; the mobile telephone switching offices support entirely different technologies. This means that redundant infrastructure will likely need to exist for as long as CDMA is still supported.

From a network perspective, some changes are relatively easy to accomplish. For example, "Purple" doesn't have its own long distance network and uses its competitors' networks to complete long distance calls. By acquiring "Yellow," they'll gain in-house long distance network capability (although this is in and of itself a sticky business question involving partially owned subsidiaries). Switching to this can be as simple as specifying a different gateway for long distance call termination (or additional routes in the dial plan). It's also possible to consolidate roaming agreements and billing arrangements with other carriers. Generally speaking, in a merger like this, the merged company will seek to maintain the most favorable agreements from each company going forward (although history shows that while cost savings may be realized, the prices charged to consumers are unlikely to change).

Other things are much more complicated. I am not worried about the newly merged company's footprint in my Central Office shrinking, at least not in the near term. And my financial plan for next year reflects the status quo. For one, there is no guarantee that the merger will happen. The federal government has yet to approve it. For two, even if approval takes place, the stuff in my Central Office is difficult and expensive to fix. The cheap, easy stuff will take at least a year to get done, and none of that work is here.

And in the meantime, key people at both companies are worried about losing their jobs. Visitors to the Central Office often ask if we're hiring. "We're hiring someone to clean Bella," I reply, gesturing forlornly to the port-a-potty in the parking lot. Thus far, nobody has taken me up on the offer. I'd say the sun-ripened odor of chemical toilet wafting across the parking lot is a character-building experience, but we have a better one here in the Central Office: Icky-Pic! Have a hackerful summer, and I'll see you again in the fall.

How to Be a Guitar Hero, IRL

by J.J. Styles
jjstyles0001@gmail.com
aka OptiKaL IlusioN

Hello, World (I just love having an audience that knows that reference!). I will attempt to make this article brief, informative, and fun. We will be discussing the electric guitar (a musical instrument device), software called “Rocksmith 2014” by Ubisoft (“Rocksmith 2014” henceforth shall be referred to as just plain old “Rocksmith” for the remainder of this article), applications used to enhance the Rocksmith experience, and an online community called CustomsForge (I would say a “fantastic” community, but that judgment is for the readers to make).

Anyone familiar with the movie *Sneakers* (1992) might recall a character named “Whistler” that can do fun and amazing things with sounds (he’s the blind hacker/phreak). Phone phreaks in particular appreciate sound manipulation the most (ever play tunes using DTMF?), but it’s tough to find a living human that doesn’t have a novahot rocker star inside their soul, waiting to be unleashed (yes, that was a Shadowrun reference).

You may hear the words “Smith” and “Forge” and “Rock” and assume that heavy metal music is the focus of this article, but that is certainly not the case. All genres of music can be played on the electric guitar, and utilizing Rocksmith. The acoustic guitar is confined to one particular sound (unless equipped with a pickup and output jack), but the electric guitar can sound like anything one can imagine. Sonic effects (digital and analog), MIDI (Musical Instrument Digital Interface) pickup interfaces, and software/apps (including plug-ins) are now more commonly used.

The guitar, invented blah blah blah (go look it up on Wikipedia!) is akin to coding in Assembly or, rather, a second generation computer programming language, especially when compared to other stringed musical instruments. Take a piano for instance (yes, there are strings inside of a piano). The piano

player interfaces with the strings through a series of “keys” and “pedals” used to generate certain specific “notes” and combinations of notes (“chords”). This interface acts as a layer, preventing the player from directly manipulating, or programming, the strings. Whereas the guitar player has direct access to the strings that generate sound, giving them the ability to pick, pluck, strike, bend, slide, and mute the strings, et cetera and so forth. This is the kind of minute detail an Assembly hacker can and should appreciate. (How does a programmer access CPU registers directly in a third generation or higher language? Don’t ask me!)

By this point, if we haven’t appealed to the inquisitive hacker side of your personality, perhaps the social and emotional benefits will persuade you to come to the rock-side (*Star Wars* analogy? Yes? No? Whatever!). Guitar players perform at gigs/shows. This is a social activity. Most social activities are dull wastes of time, but any DefCon speaker will probably tell you that being the center of attention in a peer group setting *is pretty awesome!* Praise, admiration, acceptance, chicks/dudes, booze/drugs, parties are all there waiting for you (even maybe true friends - those are rare though) if you are willing to “grab the brass ring” so to speak. Partying is a devotion to pursue, sometimes a lifelong devotion - especially when the weight of intelligence becomes too much to bear (I’m saying extra brain cells are a burden, yes).

So now that I have hopefully convinced you that the electric guitar is the superior instrument to spend one’s time with, where do we go from here? Now that you’ve acquired an electric guitar, what now? Get yourself a Realtone cable and a copy of Rocksmith 2014 for Windows, OS X, Xbox 360/One, or PS3/4. A Realtone cable is merely a quarter-inch (1/4”) left channel monaural (mono) phone jack connector (commonly referred to as a “guitar cable”) on one end and a male USB 2.0 connector plug on the other. Plug the guitar cable into your guitar, plug the USB end into the female receptacle on your Rocksmith compatible system of preference (I like to call this “jacking in”), and boot up Rocksmith.

A Realtone cable is essentially a USB guitar cable (a readily available third party item), but there is a proprietary copy protection type box device that prevents Rocksmith from functioning without an authentic Realtone cable. I have heard about custom hacked dynamically loadable library files (.DLL files) that allow the use of USB guitar cables in Rocksmith, but I use an authentic Realtone cable (we will discuss how to utilize Rocksmith without a Realtone cable at the end of this article).

In the newest version of Rocksmith (Rocksmith 2014 Remastered), there are many modules to keep a guitar player (or bass guitar player) busy for the rest of their life. “Amp” mode is where one can experiment like a rock’n’roll mad scientist, configuring combinations of amps, pedals, even virtual speaker emulation (a 15” speaker has more bass frequency than a 10” speaker and Rocksmith knows this). Once a compelling filter for the guitar to sound like has been achieved, one could venture into “Session” mode, where a virtual jam session can be started up, allowing for drums, bass guitar, and even another guitar player to provide a platform for one to “noodle around” on top of. Perhaps after this, “Lesson” mode could be activated, where videos describing various techniques can be watched. One could sit back and “load a bowl” at this point and “zone out” But rather than grabbing the bong, I would recommend continuing to hold onto that guitar and following along with the lesson vids, attempting the methods performed before you. After learning a few techniques, one could attempt to perfect those techniques in the many “Arcade” games Rocksmith has to offer. Games that focus on “chords,” “volume control,” “fret” and “string” accuracy, “scales”, and “slides” are a very rewarding and perhaps overlooked feature that can actually contribute to a guitar player’s skill level (games get you XP, IRL. Quickly. Whoa!).

Attention please: Now we shall talk about “Learn A Song” mode. This mode appears like a Guitar Hero/Rockband session at first glance. On second glance, it’s easy to ascertain that right before your eyes is actually a moving digital representation of guitar “tablature”, flying towards you like a speeding train (just like Guitar Hero/Rockband!). Rocksmith comes with a library of songs built in that can be played at varying skill levels represented by

percentages. With the “auto-level up” setting bit flipped, one can start at zero percent, and after several play-throughs, be at 100 percent. (And then she started playing “Blitzkrieg Bop” all the time, joined a band, and we never heard from her again.)

A Rocksmither could even raise their awareness to 200 percent once the song has been memorized and played with minimal assistance/cues in “Master Mode.” I would recommend doing this before playing a cover song at a gig, but that’s just a recommendation, not a requirement (maybe play it for grandma first?).

After a satisfying score has been thrown down, an insecure/competitive gamer could put their chops to the test by comparing their score to others on the online “Leaderboard” through a round of “Score Attack,” available in easy, moderate, hard, and master modes. This is not necessary, as guitar playing does not need to be competitive to be enjoyed. In fact, many guitar players refuse to judge guitar mastery through any kind of measurement system. With that said, the gamer in me is never satisfied until I achieve the #1 spot on the leaderboard (foamyandsmokey on Xbox Live!) so I don’t even bother unless confident I can wail. Perhaps I have an unfair advantage in that I have experimented with various pickup switch settings (there are five selections on my American Standard Fender Stratocaster) and various tone/volume knob settings, and have gained acute awareness of preferred combinations to utilize, achieving maximum points for note accuracy (I noticed sometimes I did not get credit/score points for hitting the correct notes and that pissed me off so bad I went OCD). Now that I have shared that knowledge, my conscience is clear. Be sure to figure out your tones before you compete against me. One could also cheat by using a digital audio workstation (DAW) such as Audacity and create a perfectly sequenced track to play through the Realtone cable (just like holding up a microphone to the speaker during karaoke mode on Guitar Hero or RockBand), but I have never, *ever!* ranked on an online leaderboard through cheating. (One time in typing class, I wrote a macro in Windows Recorder to type the alphabet backwards in less than two seconds to impress chicks, but that’s it! I don’t cheat!) And I recommend you never cheat. Because once a person cheats, any achieve-

ment they make in life will be assumed by others to be fake. Cheating is easy to detect - by people and algorithms. Whoa, it's dizzying up on that soapbox. Where was I? Oh yeah! Learn A Song mode.

Let's assume, for the sake of continuing the pace of this primer, that after a span of time has passed, our hypothetical Rocksmith has exhausted the library of songs provided with the retail copy of Rocksmith. Every song is at 200 percent completion, photographically memorized note for note, chord for chord. What now? Well, all versions of Rocksmith have DLC (downloadable content) available for a fair price (usually \$2.99 USD per song) through the usual online software dispensaries (Valve Software's Steam, Xbox Live, PSN). One particularly well priced option is the "Compatibility Kit" that imports all of the original songs from the first Rocksmith, released in 2012. The songs in this package, and all available DLC, are well indexed online, including on Wikipedia. Obviously, the online leaderboards are not as populated with other players' scores, since not every player bothers with DLC but, aside from that, everything is the same as the built in songs. I have purchased hundreds of dollars worth of DLC for my Xbox 360, which I started to regret. Whenever a "Red Ring of Death" claims the life of one of my 360s, I rip it apart and attempt to fix things, but most of the time I fail. The few times I succeeded in resuscitation, it was usually just a matter of time before the red lights came back, or something else like a laser pot needed tweaking, and I wound up just getting a new 360. When this happens, a license transfer must occur in order to use all content purchased or licensed to the previous console. License transfers have a limit on how many times a year they can be issued (I think it's every six months), so if a few systems die on you during a year (happens a lot to used/refurbished systems), things can get complicated (you can start to feel very ripped off). If the "new" console is always connected to Xbox Live, this is not an issue (the DLC can be authenticated). But during periods of no Internet access (times when you really *need* things like DLC to pass the time, waiting to save enough money to pay the Internet bill), you're just totally screwed. SOL.

It was during a period of time like this that I learned I could play Rocksmith on my

mid 2014 MacBook Pro 13" Retina running OS X Maverick release, using the Realtone cable I already owned (the breakaway Xbox adapter, didn't matter, much like the way an Xbox controller can connect to any computer). After obtaining a code from MacGameStore for \$12.00 USD (\$48.00 dollars less than the retail price and the price Steam wanted), I started the download from my temporary public Wi-Fi connection. While the bits trickled down the invisible wire, I investigated the differences between the console versions and the computer versions. I quickly found out that the Mac version of Rocksmith and the Windows version were easily modifiable, offering a whole new world of possibilities to a broke ass like me. Having already spent a small fortune on Xbox DLC, I felt completely justified in fooling around with copyrighted materials, knowing full well that recording artists, record labels, Ubisoft programmers, and even Microsoft had been compensated already (sorry Valve! But hey, I didn't use Steam's bandwidth for the DLC, so no harm no foul). Apparently, purchasing Rocksmith on Steam (and just about any game) grants access to both Mac and Windows versions of titles, but at the time I didn't have a license for Windows, so I didn't have Bootcamp installed and I completely focused on Mac. All I had to do was 1) Purchase one song, in order to have a valid license that could be spoofed from now on by other content; 2) Obtain and run a program called "RSInjector." This application contains a dynamic library file called "RSBypass.dylib" that, in a nutshell, acts as a man in the middle allowing "Rocksmith 2014.app" to run and load any ".m_psarc" files (instead of ".p_psarc files" which operate in Windows) contained in a directory stored in the "~/Library/Application Support/Steam/SteamApps/common/Rocksmith2014/dlc" folder; 3) Finally, just obtain some songs to copy into said DLC folder. The instructions for Windows are even easier. All that is required is obtaining a file called "D3DX9_42.dll" (merely a special DirectX 9 library modified to allow the loading of CDLC, with spoofed license data), copy it to the folder containing Rocksmith 2014.exe, and it's ready to go.

The following are the instructions most people go by to do what was just described:

How to Use Custom DLC (CDLC) on Mac

1. Your user account needs to be an Administrator account.
2. You need to enable third-party apps. Open System Preferences, click on "Security & Privacy", and on the General tab under "Allow apps downloaded from", choose "Anywhere"
3. Download and install Steam. It must be installed in the default location.
4. Purchase and download Rocksmith 2014.
5. Purchase the Smashing Pumpkins "Cherub Rock" DLC for Rocksmith 2014. You must buy it so that it is licensed to you. You can purchase a different RS2014 DLC if you want, but using "Cherub Rock" is the easiest as that is the default AppID used by most CDLCs here. If you choose to purchase DLC other than "Cherub Rock," *it must be RS2014 DLC*. Purchasing original Rocksmith 1 DLC will not work. You will also have to use the RS Toolkit to change the AppID of each CDLC that you download to match the official DLC that you purchased. This is why buying "Cherub Rock" is recommended.
6. Download RSInjector.
7. Place RSInjector in your Apps folder (it can actually be anywhere, but you might as well keep all your apps in one place).
8. Download the customs you want. Make sure they end in "_m.psarc". If they end in "_p.psarc" they are PC-only versions and will need to be converted with the Toolkit. I'll put instructions for that down below.
9. Place the customs in the DLC folder. The location is: "~/Library/Application Support/Steam/SteamApps/common/Rocksmith2014"
10. It is a hidden folder, so the easiest way to find it is to open Finder, and using the "Go" menu, select "Go To Folder" and paste the location in there. You can then drag the DLC folder to your sidebar to create a permanent link.
11. You can also find the folder by opening Steam and going to your games library and right-clicking on

Rocksmith 2014, and choosing "Properties". Select the "Local Files" tab and click on "Browse Local Files".

12. Open Steam, but *do not* launch Rocksmith 2014.
13. Launch RSInjector, which will automatically launch Rocksmith 2014.
14. Say goodbye to your family, friends, and free time. You won't be seeing any of them for a while.

These CDLC cracks can be performed on console gaming systems as well, but due to the fact that jail breaking techniques must be used in order to achieve what has been described, I will leave it up to you to investigate these methods, as I do not personally condone jail breaking, not do I want to be blamed for the repercussions one could face as a result of doing so (bricking your system, getting banned from online services, etc.). *Do at your own risk!* (plus that would be beyond the scope of this tutorial).

I personally do not feel like a genius computer whiz for having accomplished this trivial hack. On the contrary, I feel like an idiot for not having done it sooner. But, if I *had* done this sooner, I might have been tempted to never purchase any DLC, which is a total dick move. I still purchase DLC for my Xbox, especially for recording artists I truly appreciate and support. I like to believe that Ubisoft could fix this crack at any point by implementing a "phone home" method or any number of copy protection schemes. But rather than using intrusive countermeasures to limit their faithful users, they allow a modding community to exist and thrive (that and they probably continue to sell more copies and make even more money allowing us to continue). They can also see what is and what's going to be popular DLC to offer. I played CDLC for Bad Religion way before I purchased their songs legitimately in Rocksmith (just recently became available). Of course, these are just my speculations. I have attempted to get opinions from Ubisoft programmers on the subject using social media, but they usually stop replying to me after such inquisitions (LOL).

So now that we have a fairly complete understanding of the offerings Ubisoft has supplied the guitar playing world, let's speak about the offerings that the CustomsForge community has offered to the Rocksmith world. Currently there are 22,708 down-

loadable .psarc files indexed on <http://ignition.CustomsForge.com>.

The site has grown by at least 5,000 songs since I joined and continues to grow. Before CustomsForge was established, .psarc files were already being exchanged through the traditional underground means of transmission (still are, and still would be if CustomsForge went away). In fact, CustomsForge does not literally store any files of a copywrited/copy-written nature, merely pointers (hypertext URL links) to web-based file-sharing sites that contain them. CustomsForge does store/host/contain a social network of Rocksmith enthusiasts that participate in various ways such as forums, tutorials, .psarc file creation, .psarc file leeching, etc. I am primarily a leech and a lurker. I live an unstable lifestyle that could be easily taken away from me at any point if I were to get into trouble. Some folks can afford lawyers. I cannot. Some people are good at crowdsourcing and fundraising (for lawyer support). I am not. Some people feel they have nothing to lose. Also, I say crazy things! So when I do communicate, I try to be meaningful and have thought out ideas and questions. Usually my questions either get answered, or have already been answered. (I learned this 20 years ago in the alt.2600 FAQ! Asking stupid questions like “How do I hack?” is for n00bs, lamers, posers, and narcs.) Sometimes I attempt to solve unanswered questions for people when all replies have been from know-it-all d*cks and as*h*les, proclaiming “that’s impossible!” Luckily however, those types of people are slowly becoming extinct (except on microsoft.com forums) and virtually do not exist on CustomsForge. Whatever the case may be, the guitar wielding bodhisattvas of the world have decided to contribute and devote their skills and time to converting sheet music and tablature to .psarc files, or even figuring songs out manually through “playing by ear.” As a result, these friggin’ geniuses provide leeches like me a few minutes of nirvana, figuratively and sometimes literally (RIP Kurt!) by letting me experience my favorite art form firsthand. Though I am capable of playing rhythm guitar and bass by ear, detecting the minute intricacies of fast tempo leads and fills is a real challenge and sometimes impossible for me to figure out by ear. Plus, having a guide to follow gives me confidence (even if the guide is incorrect).

Guitar playing (like many things) is about confidence. When a person performs a task with confidence, the task will usually, more than likely, get executed smoothly. Confidence helps to free one of jitters, stutters, hiccups, flubs, blunders, bumbles, etc, and other such side effects of insecurity. Now though, people have learned that being quirky gives people character. Quirks make the world interesting, and people more relatable. If you see me on stage “butchering” a song, I’m probably doing it on purpose. Confidently! When I butcher a song, it’s either because I’m drunk (got that way on purpose!), or because I haven’t devoted my entire life to perfecting that song. Just like at a karaoke bar. At a karaoke bar, people have fun whether they can sing perfect pitch in seven octaves or not. I give people props for picking good songs, for having “tastes.”

Developing personal style makes life fun, easier, and more memorable - and playing the guitar totally helps. It pretty much forces one to build style.

So now that we have gone over some business, social, and personal discussion, let’s get back to some technical data.

The Rocksmith Realtone cable is a proprietary USB to quarter inch phono guitar jack cable. It is a fine piece of equipment and, when I say that, I mean that it is a fine POS (piece of stuff). The cable works just fine, don’t get me wrong, but I personally have owned four different cables due to breakage. These cables do not stand the test of time very well in my experience. My guitars and I spend a lot of time connected to Rocksmith, but I take care of my Realtone cables and still they break. Sometimes I can get extra use by placing extra tension on the cable by looping it from the input jack through my guitar strap, but this is a temporary fix at most. At this point, one must either purchase a new cable, which costs \$29.99 USD brand new, or look into a “no cable” hack. A no cable hack will allow one to use a nonproprietary USB to guitar cable, or even utilize a professional audio interface as an alternative sound input source for Rocksmith, or even a microphone. This is a big deal! Music audio interfaces made by M-Audio, Focusrite, etc., have lower latency (digital sound lag, like buffering) and a higher frequency range. So the signal Rocksmith can receive will be of a higher quality, meaning higher scores! You’ll finally get credit for those missed notes

that you know you nailed (the ones that make you want to smash your guitar!). I have tried several different applications to bypass the Realtone cable requirement and have experienced inconsistencies and glitches with all of them, with the exception of one program. So now I will elaborate on that one:

NoCableLauncher available at <https://github.com/Maxx53/NoCableLauncher> allows for point and click ease of use. All one must do is locate the target Rocksmith installation (standalone and Steam version) and select the appropriate sound input source. After that has been determined and the settings file has been written to disk, the next step is launching Rocksmith, which will occur automatically after a point and a click. The only other advice I have to offer is to try experimenting with the Windows Sound Mixer control panel input level settings. For example, my best input level is 10 out of 100. Once I start going past 17 out of 100, the signal becomes too distorted (over modulated) for Rocksmith to accurately determine notes. NoCableLauncher is a work in progress, and just recently (as of this article's creation) included the capability to take advantage of the multiplayer option in Rocksmith, meaning you and your bass, rhythm, and lead guitar players can jam out on separate guitars together and

get that new cover song for your band down nice and tight. Yeah!

CDLC (Custom DownLoadable Content) is the same as DLC (DownLoadable Content), but in order to use CDLC you must use a patch to modify Rocksmith. Modifications are straightforward, but I would recommend going to <http://customsforge.com/forum/151-new-customsforge-support-forums/> for assistance. The best part about CDLC (besides not having to pay for it) is that anyone can create their own CDLC. Whether you use sheet music, tablature, MIDI files, or just play by ear, creating CDLC can be very rewarding, both as a musician and as a coder/creator. RS Toolkit and Editor on Fire are software tools used to accomplish the creation of CDLC. If you need assistance using these tools, I would advise that you go to <http://customsforge.com/forum/154-cdlc-support-discussion/> and if you just want to explore all the fantastic content created by other CDLC developers I'd suggest checking out <http://ignition.customsforge.com/>.

That is all I have to offer right now. I hope you have enjoyed this article and I wish you well on all your musical and technical adventures!

EVEN RESTAURANTS NEED INFOSEC

by lg0p89

Recently I attended GrrCON, an InfoSec conference in Grand Rapids, Michigan. (Incidentally, this is one of the best InfoSec cons in the Midwest with varied talks and subject matter.) While there, the group visited a local Chinese restaurant. This had the usual layout. As we walked in, the WAPs were rather conspicuous, so we knew there was Wi-Fi. There was no posting that you see at other establishments stating "The Wi-Fi password is xxxxxx." A quick look from the phone showed the Wi-Fi present and visible. From here, the manufacturer and model was researched for the specifications and potential default password. The default password and generic guesses were attempted (e.g. admin, the restaurant name, etc.) to no avail. To get

where we needed to be, a smidgen of social engineering was required. The waitress was asked for the password, which was probably not for the public's use. Initially, she asked for my phone to key in the passcode. Gingerly, I told her with a smile "I never give out my phone."

I was a bit surprised to be asked to give my phone to a stranger to take to parts unknown in the restaurant to input the passcode and who knows what else. The waitress volunteered, as she wanted to be very helpful, to write down the code for me. A few moments later, she dropped off a napkin with the passcode (AF20171998) nicely written out. The napkin happened to be passed to a few others in the group. The protocol for the passcode appeared to be possibly the owner's initials,

the current year, and possibly the year the restaurant started.

From here, we were able to review the Wi-Fi IP, BSSID, local address, and what devices were on their network. Curiously and sadly, the restaurant's Wi-Fi was using WEP, still. This included the server, stations where the waitresses would input the orders, the cashier's station (presumably the device used to run the credit cards), the cashier's iPad, and several other devices not nearly as exciting.

A quick scan of the server showed the open ports and services. These included the Microsoft-DS (SMB directly over IP) and the MS-SQL-S (Microsoft SQL Server), among other services easily and quickly seen.

This is not an unusual occurrence in small- and, at times, medium-sized businesses in America. The small business owner, not knowing any better and not having the capital to purchase professional services, simply goes to the Big Box store to purchase items and try their best to install these or, better yet, have their cousin try. The results tend to be *not* optimum (aka poor - and amazingly insignificant to take advantage of for those in the field).

In this specific case, there were correct and incorrect protocols observed in this installation and procedure.

Correct

Although this was a rather disheartening chain of events, there were a few items that were of a more positive nature. Granted, there was Wi-Fi present, as anyone with a simple smart phone could tell with ease. The fact the restaurant management did not publicize this at the front of the restaurant as the patrons walked in was a good thing. Once you have this out in the open, the restaurant is manually beaconing its existence and handing out a welcome card to the curious. Without a slight sprinkle of social engineering, the Wi-Fi may be seen, but generally not entered, much like a massive wooden door on the front of a mansion. You can see the building and door, but you don't know what is on the other side.

Also a positive is the fact that the password itself did not appear to be static. From the naming protocol, it appears that the year would change annually. Although this is

only an annual update, it's clearly better than nothing.

Those are two of the positive points. Alternatively, there are a few ways they could have improved the situation so they would not be as vulnerable to the InfoSec public.

Incorrect

Although the food was good, the security, unfortunately, was not. The patron/guest network really should be different. When you allow the guests access to your network where your business hardware is located, such as a waitress station where they enter the food orders, there may be an issue if someone is bored and has rudimentary equipment. As a business owner, you are asking for problem. Don't do it.

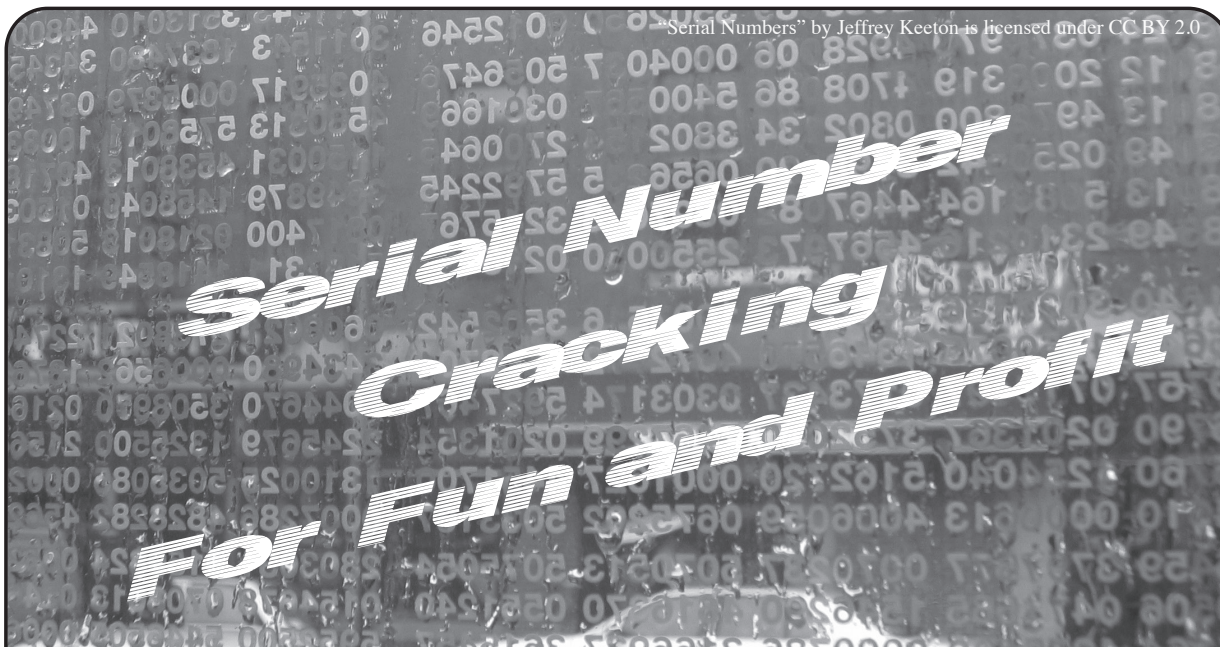
Let's say you don't want people connecting to the Wi-Fi. Don't give out the passcode. It is simply that simple. As a small business owner, you probably don't want me connecting to the Wi-Fi when you have everything else connected.

Last, but certainly not least, keep your Wi-Fi protocols up to date. This does not need to be the cutting edge and it doesn't mean adopting everything just as it comes out. If you want, just wait a bit until any potential issues have been vetted by the community at large. In this case, WEP was being fully implemented for not only the restaurant, but anyone connecting to the Wi-Fi. There is no need to expand on the inadequacies of WEP at this point. What is pertinent, however, is that WPA2 should have been in place and used, if not for the welfare of the patrons, then for the restaurant's operations and welfare.

With the rudimentary issues resolved, and without taking a massive amount of time, energy, or expense, security could have been applied in at least a baseline level. Even with this in place, the establishment would be a bit more secure and less likely to be popped, along with the customer's personally identifiable information (PII).

In Closing...

If you are a small business, or if you consult with small businesses, please make sure their technology is relatively up to date. Without this covered, the business will be at risk.



by MrGhostValley

Like any student of social engineering, I'm fascinated by speculative bubbles. That hype alone could cause people to act in ways they would themselves otherwise consider irrational is remarkable. Greed and fear can drive humans to do some pretty wild things - and generally, somebody stands to profit. And while, like many of you, I channel most of this fascination towards cryptocurrencies, I've been keeping a keen eye on something with even better returns. In these strange times, elite marijuana seeds have come to fetch absurd sums in private online auctions - up to \$2,500 for a small packet of ten seeds.

There are huge sums of money involved, but the nature of the product is such that the buyer can't possibly know the contents. First, all cannabis seeds are virtually identical. Second - and more importantly - the buyer has no way of knowing if the seeds were what he paid for until he (and it seems in this high dollar crowd, it's nearly always a he) has grown them out for at least two and a half months. On top of that, the packaging is generally impromptu - a heat sealed Mylar envelope, or paper packet. And because the auctioneers are entirely used to offering products from private collectors, there's a serious vulnerability to unscrupulous actors auctioning off counterfeits.

Enter a third-party with a pretty good idea. We'll call them CannProve [not their actual name]. For ten cents apiece, they'll sell the original producers a specialized tamperproof label to place over their otherwise easy-to-

knockoff packaging. One end of the label has a holographic CannProve logo, while the other end has a unique serial number and a QR code. If anyone wants to verify the authenticity of a pack of seeds using a CannProve seal, they confirm that the seal hasn't been broken, and simply scan the QR code to be brought to a web page that lists information about the individual package. It's a neat mechanism that introduces a basic level of trust. Unfortunately, that trust mechanism is all too basic, because it can be exploited. A motivated attacker would size the challenge up against the payday - counterfeiting a mere six packs could yield enough money to buy a car. And, unlike trying to profit off a counterfeit Visa card or Coach bag, this whole transaction operates without visibility to authorities. A motivated attacker, in other words, would be within reason to apply some time and effort to this problem.

First, some Open Source Intelligence (OSInt). A quick Instagram search of the producers fetching top dollar at auction would reveal a photo of a strip of CannProve labels before they've been applied to packages - just a friendly assurance to potential consumers that the products are verifiable. Our attacker would pull it up on a laptop to zoom in for some clues. First, the attacker would learn the format of the serial number: a six-digit number, followed by two alphabetic characters - for example, 102015JG. After looking at a second, the attacker would notice the numeric portion is sequential, but the alphabetic is pseudo-random: after 102015JG comes 102016CS. Looking at the five labels present in the photo,

the attacker wouldn't be able to discern the hashing or algorithm to produce the two alphabetic characters from given numbers, but then there's the last clue. The attacker would scan a QR code and be brought to the verification page located at <https://cannprove.com/prove/102016CS>.

The attacker would realize instantly that the serial numbers are all available in the public facing URLs being served by CannProve.

Armed with only the valid serials, the attacker could generate QR codes and counterfeit labels that would scan and verify. CannProve could have prevented this - or at least made it quite a lot more difficult - by using non-sequential pseudo-random serial numbers and hashing them for their URLs. But they did not.

First, the attacker would have to pull a list of valid serial numbers. He could do this by sequentially iterating through URLs in <https://cannprove.com/prove/> and checking the contents for a phrase that appears only on valid pages (such as "CannProven!"), and write the pages that meet this criteria to a file.

He could do this very quickly and easily with a simple bash script, like this:

```
#!/bin/bash

START=${START:-2000}
END=${END:-4999}
# call like this to adjust defaults
# START=2000 END=2001 bash hunter-gatherer.sh

echo -e "Good Serialz:\n" > good_serialz.txt

save_if_good () {
    local this_serial="$1"

    curl -sL "https://www.cannprove.com/prove/${this_serial}" \
        | grep -q 'CannProven!' \
        && echo ${this_serial} >> good_serialz.txt
}

wait_for_jobs_to_complete () {
    for job in `jobs -p`;do
        wait $job
    done
}

for num in `seq ${START} ${END}`; do
    time=$(date +"%T")
    echo "$time: Downloading Set 10$num"

    for a in {A..Z}; do
        for b in {A..Z}; do
            this_serial="10${num}${a}${b}"

            save_if_good "${this_serial}" &
        done
    done
    wait_for_jobs_to_complete
done
# remove for more parallelisim (probably blow up your system
➡ file handle limits)
wait_for_jobs_to_complete
done
wait_for_jobs_to_complete

cat good_serialz.txt
```

The motivated attacker would order the basic packaging components from Amazon, use further Instagram/Google image searches to capture detailed images of the labeling, and print the front stickers for the packaging at a local copy shop.

Now with only the seal to spoof, the motivated attacker would be left with a few possible options. First, given the value of a successful counterfeit, the motivated attacker could spend less than \$5,000 to order genuine holograms with all of the related security features of the original. While this might typically be difficult to discover, Instagram once again provides high quality close-up photos of enough samples to derive the full set of security features in the hologram. This approach would be ideal and virtually impossible to detect and, although the cost could be prohibitive, the return on investment could still be massive.

In the case of limited funds, a DIY attacker would have to get creative. First, examining the photos available under the #CannProve hashtag on Instagram, the attacker would notice the QR code labels in various photos with objects that can be used to determine scale and size. The proper sized round-edge square metallic labels could be purchased from Amazon and then be printed with the derived serial numbers and associated QR codes. This still leaves the attacker with the hologram to defeat. Thankfully, Instagram saves again. A little research shows that the producer fetching the highest auction bids places the QR code portion of the label to the front and actually places a white mailing label with text over the hologram.

The challenge is simplified for the attacker: nearly any hologram sticker cut to size will do because it will be mostly obscured with a white label. Few people take the time to inspect holographic seals, and a proper inspection is impossible in online photos. Perfect? Not by any means. But the photo posted to the auction will have a working QR code that will validate as the correct item.

The motivated attacker could perform the DIY attack in just a couple of days and the more impervious attack in about six weeks given the lead time on the holographic labels. By placing all of their trust in a single security label, the producers, auctioneers, and consumers leave themselves vulnerable to a savvy attacker who could be long gone with

six figures before anyone could verify the authenticity of the merchandise by growing it.

Security Lessons

First: Use randomness to make things hard to guess.

One major weakness of this trust mechanism is the sequential nature of the serial numbers. If they were longer randomized identifiers, such a brute force collection method as the BASH script would become completely impractical. You should consider this any time you need to secure something in a way that could be either patterned or random: patterns are easier to observe, easier to guess, easier to remember, and easier to process computationally.

Second: Protect and obfuscate identifying information - dividing it into pieces makes total compromise less likely.

In this case, the QR codes should be pointed to URLs based on hashes of the serial numbers, not of the serial numbers themselves. This would completely prevent any possibility of connecting the hash derived from the URL with a valid serial number. As is, if an attacker gets one, he or she has both. In your personal life, this means everything from taking precautions like removing the labels from old shipping packages before recycling them to using two-factor authentication so your password isn't a single point of failure.

Third: Social media is a public record. Think before you share.

If you post a picture of anything that you rely on for security to social media, that genie is out of the bottle. Here, the images of the packaging and the labels are what give an attacker the basic information to craft the ploy. The detailed photos of holograms showing off their neat security features are *exactly what make them susceptible to mass duplication. The same goes for your ID badges, notes with passwords, even photos of your keys.*

Fourth: Security features can at least slow and potentially stop even a motivated attacker, but not if you disable them.

A producer who covers the security features on his or her label, a business that doesn't arm its alarm, a motorist who doesn't lock his car doors when he parks at night - these are easy prey and will eventually be taken, especially if the target is valuable enough.

AUTOMATING A POLICE STATE

by Corey Kahler

When my wife received her first red-light camera ticket for failure to stop, both she and I immediately said it was impossible. No, of course it must be a problem with the automation system.

In Seattle, automated tickets come with a video link showing the infraction. Pulling it up, clear as day, my wife had California-stopped at a right turn - not completing a stop on a red and treating it more like a yield - and had technically run the light. Ticket paid.

Obviously, most folks hate these cameras, and it's not only because they automatically catch us making the tiny slip-ups that are generally forgivable which we would rather not have on our record. There are generally two main complaints beyond ego.

The first is that a human police officer should be allowed to make a judgment call on whether a ticket is warranted - the prototypical, being left off with just a warning.

Additionally, officers performing traffic stops can also discover other things - the smell of drugs, suspicious behavior, broken tail lights. Granted, red light cameras can take officer's discretion out of a clear cut situation, leading to a reduction in perceived bias or racism.

The second complaint is that automated ticket cameras are there only to make money. Tickets come in and there's indisputable evidence, so pay up and car patrols have to do less work.

This frustration is similarly aimed at end of the month heavy ticketing or speed traps that most American drivers are always aware of. Point being - cops are ticketing for their own interests, not the public safety.

I would like to introduce a third complaint: normalization of the automation

of a police state.

Consider: Should cameras be allowed to check our tabs as we drive through intersections? Should it scan every license plate for proof of insurance? Generally, should your car, regardless of committing a crime, be constantly monitored for adherence to the law?

This isn't to say that automatic cameras haven't done some good. There are plenty of cases where cameras allow the police to support or deny alibis, document wrecks to determine fault, and see victims in need of assistance.

However, in those cases, the value of the cameras was incidental - not programmatic.

Take it a step further - roads monitored for speed violations based on your car's GPS. Google Maps and the aggregated data of self-driving vehicles will eventually know the speed limit on most roads. A GPS-connected vehicle follows your speed just like when you take a jog with a FitBit. So why not - if you go too fast for that area - allow you to be immediately reported and ticketed?

For current technology, this is not a huge leap.

While self-driving cars may have some control of the speed and be responsible for it at a later date, in the meantime, what can be said about a system that can track your speed and location and check your records whenever possible? And if we're fine with automation checking our speed on highways and the completeness of our stops, why not this? After all, you should always follow the law, right?

Can't we say that automation leads us more towards a police state than actually having more police watching us drive down the street?

The Hacker Perspective

by Christy Ramsey

My college completely replaced its computer system. Gone were punch cards and the stacks of paper cascading through metal benches. Instead, plastic globes embedded with shiny glass and keyboards drew me into their orbit and I spent years exploring the world of Digital Equipment Corporation and its PDP 11/70.

The very name Digital Equipment Corporation (DEC) invited investigation. Their computer systems were named "PDP" which stood for Programmable Data Processor, which is a description of a computer (as was "digital equipment"). But bankers didn't give loans to computer companies when DEC was starting up, so the computer makers at DEC got financing for Programmable Data Processors by Digital Equipment Corporation instead. They gave the banks an Easter Egg with a computer company hidden inside.

Many DEC PDP 11/70 operating system programs were written in BASIC. *101 BASIC computer games* indeed! Sweet. Even better, the sysops were learning the new system along with the students. The race between who could explore and claim the uncharted system first was on! The crown of King of Computer Lab passed back and forth daily, sometimes hourly, as new exploits were set free by student pioneers and then corralled by the settlers in the staff office.

PIP

DEC continued the word play by naming their system's copy program PIP, Peripheral Interchange Program (never say the c-word!). Lazy students discovered that instead of laboriously retyping a friend's programming assignment printout into their own account, they could just PIP and print! In minutes, the homework was at the printer with their own account number attached. More time for creative computing or fraternity fun.

Sadly, the student copying was poorly hidden; having a dozen programs turned in with the same formatting and variable names soon tipped off the professors. One got the system administrators to remove student access to PIP. Back to typing from printouts while parties were rocking and unexplored computer vistas beckoned? *No!* Remember: the operating system programs, including PIP, were written in BASIC. I could

program in BASIC. So I started working on a BASIC program to copy files from one account to another.

I thought I was busted when a professor shoulder surfed my work. I tensed as he pointed to the heart of my copying code on the screen. He said, "Good job. You need *LINE* INPUT instead of INPUT here." Hackers help each other along the way. After applying his addition, the code worked. I lowered the permissions so that anyone could execute it and PIP was back! His help was multiplied to help many tired typists.

I kept the name PIP to reduce the mental load for some of our easily confused computer-using students. (They often were coming from or going to football practice - we all have our strengths and weaknesses.) Keeping the name the same eased "customer support" requests but also attracted the attention of a system administrator. She burst into computer lab demanding, "*Who is running PIP?!*" I calmly turned to her and confessed, "I am. It's my own copying program since the system PIP doesn't work anymore." As if I didn't know why "it didn't work anymore." She glared at me. There was no rule about writing programs; that is what we were supposed to be learning. To break her stare, I offered a compromise: "I could change the name...." She left the room. In a couple of days, PIP access was quietly restored to students. Hackers fix what doesn't work.

Limits

In the late seventies, computer storage space was expensive and therefore scarce. To encourage students to be thrifty yet allow them to work on large projects, storage limits were only checked and quotas enforced only when a user logged out. One could work with large data files and save temporary files while logged in at the computer terminal, but the sign out process checked users to make sure they were under their storage quota before logging off.

The computer club had wrangled a shared account for games which was constantly just below the quota limit. This meant the last person out of the account before the lab closed had to delete saved games or scratch files or even (horrors) game programs so the account could

be logged off and locked. At closing time one night, I was dreading the shared club account cleaning; deleting files is not a hacker value. So I raced to get off the club shared account before a friend could close out, so I could stick her with the custodian job. Don't judge me, she was doing the same, both of us smirking at each other as we knew without speaking the rules and the stakes of the contest.

Well, we thought we knew the stakes. We both logged off without clearing out the account! What? We were way over the limit. We left the closed lab swearing to each other we had not deleted files. The next day, before logging in, we did a directory of the account and confirmed we had closed the account while over quota. Could nearly simultaneous log outs defeat the quota check? The first college level synchronized keyboarding team was born. Soon curious students wondered at our practice sessions: two students with their fingers hovering over RETURN (not ENTER back then) counting down before stabbing the key on *Go!* After practicing, any pair of us could log out over quota every time.

After betting the computer director we could sign off while over quota, we showed him what a little teamwork could do. He paid up and got DEC engineers to fly in and fix the bug. Due to our revelation, every DEC system in the nation was patched. No longer did PDPs simply check to see if any other users were logged in as part of the log out process. This method allowed two signing off users to "vouch" for each other concurrently. Instead, the system set a counter that tracked the number of users logged into an account, the log off decremented the counter, and the user who pulled it down to zero had to be under quota to log out. The supervisor sent a memo to every user telling them their over quota days were over. We didn't mind. We didn't need the space and it was rude to take scarce resources belonging to all. Besides... we had other ways around the quota if we needed them.

Presidential Pardon

Remember those teletype terminals? The metal benches that squatted over piles of paper? The college administration decided to establish a satellite computer lab in a classroom building about 500 yards from the computer lab which was in the basement of the library. Not wanting to waste equipment or buy additional TeleVideo terminals, those sad old paper spewing benches with keyboards were exiled to a large closet under the stairs in the classroom building. They were linked by wire thrown into a shallow trench between the library and closet which was then covered with dirt. No grounding. No shielding.

No conduit. No joy. Every time a leaf rustled or clouds bumped, the connection was lost and had to be reset. Students soon learned that the steam-punk single line limited terminals were now not just slow, but often dead. No one used them. The staff complained about the work it took to keep old terminals in any empty room connected. They were ignored. I guess having a second computer lab to brag about without any additional cost was worth grumbling from the support staff even if it was unused.

The satellite lab did have two advantages. One was no waiting or time limit for terminal use. No one was there. This was also the second advantage. No. One. Was. There. Not only were students not in the building, there was *no* staff in the evening. So no one shoulder surfing your code (see above). The computer aides and supervisors were 500 yards and four doors away. So even if you popped up on the status monitor, you had plenty of time for a getaway, assuming your activities were worth leaving the comfy library to investigate. Faced with chasing one stray or shepherding the corralled herd, supervisors rarely left the ranch house.

One night I was working on a project in my private computer lair. The door opened. This had never happened. Stay calm, someone is probably just lost. It was the president of the college. This may be bad, I thought, he probably isn't lost. But I smiled and said, "Hello." Why not? I wasn't breaking any rules as far as he knew. Mostly, because they hadn't made computer rules yet.

The president boomed out a way-too-loud greeting for a nearly empty closet: "Hello! Glad to see you working in here. How is the lab working out?" I bet he was glad to see me. I wondered how many times he had found an empty room, probably every other time. I thought, here's my chance to speak truth to power and to practice the hacker ethic when caught: don't retreat, charge!

"Well," thinking quickly, "they aren't really used. You see, there is no supervision here. If a student gets stuck, there is no one to help." I wanted to frame the lack of supervision as a lost opportunity for help and learning for this poor lonely student, me... not have him wonder what other opportunities I could find with no supervision. I also was hoping for some extra hours since I was one of the computer aides. Maybe I could get paid to be in my private computer lair. Go big or go home. And I lived on campus, so home was not an option.

He left abruptly. It was only after he left that I noticed I wasn't breathing.

The next day, I came into the main computer lab in the library and found the benches were back! The supervisor told me he didn't under-

stand it; he had been complaining for weeks with no result, but that day the old terminals were just brought back from the classroom building without explanation.

I was happy to explain. "Oh, I told the president last night the classroom lab just wasn't working out. You're welcome." I had lost my private computer lair, but the look on his face was almost worth it. I didn't investigate whether the terminals returned so lone students could get help or to prevent lone students from helping themselves.

It's a Trap!

I went back to my college about a decade after the exploits and had a tour of the completely rebuilt computer center. I pressed the supervisor about the current balance between freedom and security. He admitted that there was one way a student could not only get banned from the computer but expelled from the college: if a "password grabber" program was found on their account.

I didn't have to ask what that was. I had written the first one on the system. Thankfully, they had not thought to make that rule back then. Although, I wondered if I should ask if they would name the rule after me, like other alumni had plaques or buildings dedicated to them. Probably best I didn't pursue the honor.

The password grabber started with ringing bells on the printer. Some student watching the system status screens discovered that printing was done with something then called "pseudo-keyboards." "Virtual" would be the term today. These keyboards could be attached to devices other than your own terminal, like a printer, to control that device. The first exploit was to send ^G (ASCII Code 07) to a pseudo-keyboard attached to the printer. In the ASCII standard, ^G is defined as BEL, which made a beep or ding: a *bell*. Later, I learned how to rapidly turn on and off the single toned beep to match the frequency of notes and play a little melody, but at the time, we were limited to trying to time the commands to have the printer play a single note version of Jingle Bells, more or less. The "line printer jukebox" effort did not get good reviews among the music critics trying to program in the lab.

After the complaints became greater than the giggles, which was nearly instantaneously, I thought about other system devices that pseudo-keyboards could be attached to. I realized that devices included every terminal including the ones the staff used to login as administrator. In fact, pseudo-keyboards could do more with terminals than ring a bell, they could display text - like the text in a standard log off message

and the system login prompt. Since the system login program was written in BASIC, the display output could be matched by a BASIC program. I knew BASIC. With INPUT replaced by INKEY\$ for password entry (so "stars" could be displayed instead of typed password characters), a write of the entered credentials to a file, and, after printing the standard "Invalid login. Please try again.", an exit to the real login program, I had a password grabber.

Since there was no fear of expulsion in those days, and I had a friendly helper/competitor relationship with the staff, I showed the director the abilities of pseudo-keyboards beyond beeping the printer. This added some drama to his every login. From then on, he started every login by first savagely jamming down CTRL-C and filling the screen with ^Cs, sometimes with a victorious chuckle. After all, a ^C stops the execution of processes and BASIC programs such as my password grabber, which then returns the terminal to system control.

I was a little sad at the brief life of my password grabber. ^C seemed a little like cheating; it was too easy to break a program. (Breaking password grabbers is why some systems require CTRL-ALT-DEL, a descendant of ^C, before logging on today.)

In my sadness, I wondered why system programs written in BASIC didn't break with ^C. Searching the manuals, I found that the system offered a ^C trap that sent execution to a special handler in the program instead of stopping the program. Another ^C would break the handler execution... *unless the first thing the handler did was re-enable the ^C trap*. I never used the ^C proof program or shared it; I didn't want to risk it getting out. Besides, it would have ruined the joy the director's login finger dance gave us. He was happy he outsmarted me. I was happy knowing he just thought he did.

I was glad to have the opportunity and time to explore a new computer system. By being helpful on various projects, sharing what I found with the administrators, and even working at the computer center, my hacking was viewed as exploring and learning, not as a threat to system security, other students, or the college. I hope the hacker ethos of helping others use computer (and other) systems even better than their makers planned continues to make online and real life more efficient, helpful, happy, and secure.

The author can be found at the nonprofit ComputerCorps in Nevada recycling, refurbishing, and repairing old electronics with other Golden Geeks and training the next generation of hackers.



Brute Forcing a Car Door with Math

by Br@d

I have a vehicle that has a keypad on the door to unlock it. When the correct five numbers (ranging from 0-9) are entered, the doors unlock. In a perfect world, I would be pretty comfortable with this feature given that 10^5 means that there are up to 100,000 different key combinations. A thief would need to try all of these to gain access to my vehicle without breaking a window or setting off an alarm. Since these 100,000 codes are five digits long, a thief could potentially have to press 500,000 keys ($100,000 \times 5$) before finding the correct one. Overall, it sounds pretty safe and very unlikely that they will guess your code, right? Wrong!

Upon further inspection, I discovered that it is far too easy to crack the code. In the following paragraphs, I will describe how I was able to figure out a method to easily and reliably crack the code on my own vehicle. Before I go any further, it is time for the obligatory disclaimer:

Simply put, don't be evil or stupid. You are responsible for your own actions. The purpose of this article is to share knowledge and bring awareness to some flaws in the design of these systems.

The first flaw in the perceived difficulty is the number of keys used to determine the number of possible unique codes. Initially, I conjectured that there are 100,000 possible codes that could be used to unlock the door.

This came from the fact that the keypad lists the numbers 0-9. However, I have yet to see a vehicle with ten buttons; most have five buttons with two numbers on each. In my case, the first button is numbers 1 and 2, while the last is 9 and 0 (you can fill in the blanks). Adjusting to account for five buttons rather than ten, we discover that our 100,000 codes have been drastically reduced to a mere 3125 (5^5). In turn, this also drops the 500,000 key presses down to only 15,625 (3125×5). But wait, it gets worse.

When playing with the keypad on my vehicle, I noticed that there was no means to "submit" the PIN when entered. As soon as the correct five-key combination was pressed, the doors would automatically unlock. This means that you can press many wrong keys prior to entering the right ones, and it will still unlock when the right sequence is entered. This seems like a major design flaw and got me thinking that there is probably a more efficient method to exploit rather than trying all 3125 combinations one after another. It would take just over two hours of endless pressing at a rate of two keys per second ($15625/2$ seconds = 7812.5, $7812.5/3600$ (seconds in an hour) = 2.17 hours) with a potential waiting time of 17 plus hours ($3125/3$ failed attempts before the timeout is invoked = 1041.66×60 second timeout = 62499.6, $62499.6/3600$ = 17.361 hours), although not all vehicles have a timeout function. This is where my research introduced me to the De Bruijn sequence

(https://en.wikipedia.org/wiki/De_Bruijn_sequence).

In a nutshell, the De Bruijn sequence is an algorithm that creates a continuous string based on the inputted values and covers every possible combination without repeating any of them. In my case, I am dealing with a five-digit PIN that consists of five possible keys. For example, the string 1234567890 would require you to press ten keys, but actually cover six different five-digit codes:

12345
23456
34567
45678
56789
67890

saving you the time of having to enter 20 of the needed keys ($5 \times 6 = 30$, $30 - 10 = 20$).

The codes for the vehicle are expressed by ten numbers (0-9), but only five different keys are needed to perform a very basic conversion to use the De Bruijn Sequence. Instead of thinking of the values of 0-9, I needed to perceive the codes as key presses. This means that the [1/2] button now has a value of “0,” the [3/4] is now “1,” [5/6] gets “2,” [7/8] is now “3,” and finally, [9/0] is represented as a “4.”

At this point, having reduced the input values down to five digits (0-4), I would love to tell you that I wrote some amazing script to generate the sequence needed for my scenario, but why reinvent the wheel? Instead, I used my Google-Fu to find an online generator (<http://www.hakank.org/comb/debruijn.cgi>). To use this generator, you simply enter the number of possible digits (1-10) for the “k” value (five in my example) and the length of the code for “n” (again, five in my case). Once the values are submitted, the sequence is generated. The following output is the 3129-digit string that covers all 3125 possible codes (15,625 key presses) based on my five-digit and five keycode requirements:

00000100002000030000400011000120
00130001400021000220002300024000
31000320003300034000410004200043
00044001010010200103001040011100
11200113001140012100122001230012
4001310013200133001340014100142
00143001440020100202002030020400
21100212002130021400221002220022

30022400231002320023300234002410
0242002430024400301003020030300
30400311003120031300314003210032
20032300324003310033200333003340
03410034200343003440040100402004
03004040041100412004130041400421
00422004230042400431004320043300
43400441004420044300444010110101
20101301014010210102201023010240
10310103201033010340104101042010
43010440110201103011040111101112
01113011140112101122011230112401
13101132011330113401141011420114
30114401202012030120401211012120
12130121401221012220122301224012
31012320123301234012410124201243
01244013020130301304013110131201
31301314013210132201323013240133
10133201333013340134101342013430
13440140201403014040141101412014
13014140142101422014230142401431
01432014330143401441014420144301
44402021020220202302024020310203
20203302034020410204202043020440
21030210402111021120211302114021
21021220212302124021310213202133
02134021410214202143021440220302
20402211022120221302214022210222
20222302224022310223202233022340
2241022420224302244023030230402
31102312023130231402321023220232
30232402331023320233302334023410
23420234302344024030240402411024
12024130241402421024220242302424
0243102432024330243402441024420
24430244403031030320303303034030
41030420304303044031040311103112
03113031140312103122031230312403
13103132031330313403141031420314
30314403204032110321203213032140
32210322203223032240323103232032
33032340324103242032430324403304
03311033120331303314033210332203
32303324033310333203333033340334
1033420334303344034040341103412
03413034140342103422034230342403
43103432034330343403441034420344
30344404041040420404304044041110
4112041130411404121041220412304
12404131041320413304134041410414
20414304144042110421204213042140
42210422204223042240423104232042
33042340424104242042430424404311
04312043130431404321043220432304
32404331043320433304334043410434
20434304344044110441204413044140
44210442204423044240443104432044
33044340444104442044430444411111
21111311114111221112311124111321
11331113411142111431114411212112
13112141122211223112241123211233
11234112421124311244113121131311
31411322113231132411332113331133


```

41134211343113441141211413114141
14221142311424114321143311434114
42114431144412122121231212412132
12133121341214212143121441221312
21412222122231222412232122331223
41224212243122441231312314123221
23231232412332123331233412342123
43123441241312414124221242312424
12432124331243412442124431244413
13213133131341314213143131441321
41322213223132241323213233132341
32421324313244133141332213323133
24133321333313334133421334313344
1341413422134231342413432134331
34341344213443134441414214143141
44142221422314224142321423314234
14242142431424414322143231432414
33214333143341434214343143441442
2144231442414432144331443414442
1444314444222232222422233222342
22432224422323223242233322334223
43223442242322424224332243422443
22444232332323423243232442332423-
33323334233432334423424234332343
42344323444242432424424333243342
43432434424433244342444324444333
33433344334343344434344344444000

```

This beautiful string of numbers might be a bit much for the average mortal to memorize, but it can easily be printed on a single side of a sheet of paper using a decent sized font.

The average person should be able to enter this sequence in 26 minutes or less, given an average of two keys pressed per second ($3129/2 = 1564.5/60 = 26.075$). Unfortunately, most cars that have these door keypads have some form of timeout system in place, but there are a number of vehicles from the mid 2000s and earlier that didn't have that option. My vehicle (a 2015 Ford) does have a timeout of around 60 seconds, but it only kicks in after 35 keys have been pressed. By breaking the sequence down to 35-digit long chunks you could go through the process in 90 attempts ($3129/35 = 89.4$). However, the whole idea behind using the De Bruijn Sequence is to cover all possible combinations in a single string. To ensure that no combinations are missed, the string not only needs to be broken down into 35-digit-long segments, but we need to start each line with the last four digits of the previous one.

To solve this new requirement, I had to get a little help from the forums (as my scripting skills are still extremely noobish). The end

result was this little pearl of script that takes 35 character length sub-strings from the sequence, where each sub-string starts 31 characters on from the start of the previous sub-string.

```

#!/usr/bin/perl

my $sequence = "<copy the
➡ sequence here>";
my $length = length $sequence;

for ( my $i = 0; $i < $length;
➡ $i += 31 ) {
    print substr($sequence, $i, 35)
➡ . "\n";
}

```

The output from this script produced 100 strings of 35 characters and a single 29 character string, making a total of only 3506 total key presses - a far cry from the original 15,625 needed to enter every possible code. This takes the original 29 minutes or less for vehicles without the timeout function to approximately 2 hours and 9 minutes, which is a tenth of the time that it would take without the sequence and no timeout! (35 characters at a rate of two per second = 17.5 seconds plus the 60 second timeout = 77.5 seconds multiplied by 101 attempts = 7827.5 minus the last 60 seconds = 7767.5 divided by 60 = 129.45 minutes or two hours and nine minutes).

I am sure that there are many of you reading this and thinking, "Hey, this is pretty cool, but also impractical" and you do have a valid point. The average crook is not going to stand by a car door for 30 to 120 minutes. They are going to do a smash and grab. However, if you think in a more devious and targeted way, there are numerous uses for this besides car theft. For example, if the target has a high-ranking position at Evil Corp, you can do your recon and figure out what they drive and where they park. You might want to gain access to their vehicle to scope it out for other valuable info or to plant a bug, but you do not want to tip them off (smashed window). You can use as many of the segments at a time as you feel safe doing during the business day to gain access. If you do not succeed on the first try, you can return on another day and continue right where you left off.

I hope that you have found this little writeup informative. Until next time, happy hacking.

Hack(ed), the Earth

by Michaleen Garda
michaleen.garda@openmailbox.org

Has anyone else noticed that it is now *required* to possess a telephone, and specifically a *cell* phone in order to access Google, Facebook, and all other “major” Internet sites? When did this happen? If a major announcement was made, I, along with most other people, missed it.

I had accounts on both sites since they were first started that I used for perfectly legal reasons, and now over a decade of personal data is lost to me because I simply refuse to use my or anyone else’s phone to connect to the Internet. Because when I began using these services, there was no clue that one day they would be removed if I refused to disclose my physical location.

I am not alone in this. Some serious Duck-DuckGo searches later, I discovered that this is a real situation. People have been locked out of their accounts with no option to verify their account except a phone. I can still buy a burner phone, but unless I keep the number, the sites will just “re-verify” later and, without access to the number, I would be lost. And I have a strong feeling burner phones will not be available for that much longer.

What does this all mean? My thoughts turn to the Arab Spring, to Edward Snowden, and finally to AI.

The Arab Spring is a name given to the phenomena of many Arabs using Facebook to enact social change. The Arab Spring was only possible because of the (then) pseudo-anonymity of Facebook. This is because when oppressive regimes can pinpoint exactly who is causing social change (like with a cell phone, for example), they can easily silence the dissenters and no social change is possible. So Facebook demanding a cell phone ensures that no group can ever use Facebook again to organize against a repressive regime safely. That is some hot coffee for you.

A lively discussion occurred with a friend where he was demanding to know why I cared

so much if we could no longer use the Internet anonymously. What do I have to hide that I am so concerned with all of our cell phones being wiretaps (as Edward Snowden revealed)? I tried to explain what a “principle” was and “liberty” and “privacy,” but he is quite a bit younger than me and never actually lived in a world with privacy, so he needed a better example.

Lord Petyr Baelish taught me to assume the worst possible motivations of others first and to see how well they fit the given evidence. I taught myself to imagine what I would do if I were in their position. So here we go - hypothesis time.

The NSA/Illuminati/whatever are sucking up every data stream on the planet, including voice from cell phones. They have been for some time. “So what,” my friend says. “You have done nothing wrong,” and he is correct. I am a privacy advocate because I am worried about tomorrow, not today. There *will* come a time when all of the data on earth is centralized and easily accessible to those in power. That data will reach all the way back to the start of the Internet. Every conversation, every friend, every location, every address, absolutely *everything* about you will be known and there really will be no escape.

At that point, the “Thought Police” will have taken over and I could be arrested just for having known someone who did something wrong. Guilt by association. I don’t want any part of this New World Order. If that means I cannot have a controversial conversation online or around any cell phones, so be it. I will be silent until it is no longer harmful to myself or others to be so. There are still some few forms of anonymity left and I value them more than what is left of the inter-webs.

And AI? Yes, AI. There are many reports of hordes of bots imitating humans all over the Internet. Maybe that is why you need a cell phone now? Wishful thinking. I am inclined to think an added bonus of forcing us all to lose our privacy is that it would make any masquerading AIs much easier to detect. I view this as an ancillary goal, unless of course that is the real goal because AI is already here. And even if AI does not turn out to be the revolution people like Tesla fear, it will still be the perfect tool to manipulate, sift, and categorize all of earth’s global data.

Enjoy yourself, it’s later than you think.



SECUREDROP

Share and accept documents securely.

SecureDrop is an open source whistleblower submission system that media organizations can install to securely accept documents from anonymous sources. It was originally coded by the late Aaron Swartz and is now managed by Freedom of the Press Foundation.

Do you have a leak or a tip that you want to share with us securely? Now, for the first time ever, you can!

2600 is using SecureDrop for the submission of sensitive material - while preserving your anonymity.

Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser, attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see.

For all the specifics, visit <https://www.2600.com/securedrop> (you can see this page from any browser). For more details on SecureDrop itself, visit <https://securedrop.org>.

SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.



Submit for the first time

If this is your first time submitting to journalists, start here.

 **SUBMIT DOCUMENTS**

Already submitted something?

If you have already submitted to journalists, log in here to check for responses.

 **CHECK FOR A RESPONSE**

ROUTINES

Creative Applications

Dear 2600:

I recently bought my first issue of *2600* in years. I chose the online Google Play edition. It was the best couple bucks I've spent in a long time, and it rekindled my love of reading. As a hacker, I had to hack the magazine like I had to hack everything else. I run Kali Linux, and it has horrible support for Adobe Acrobat, and the newest *2600* issue didn't come in PDF either. I discovered several Google Chrome extensions that could run on Linux and could turn any PDF or other web document into an audio book (using text to speech). The very best one is called "Voice Instead." It has so many options for natural sounding voices and is totally free. It even comes with IBM Watson voices! So if you are like me and collect PDF computer manuals you never get around to reading, you might want to try this. I didn't have anything to do today so I've been "reading" up on assembly, Keven Mitnick, and *2600*. I hope you will have as much fun as I have been having. Ooh, and Volume 33 of *2600* is even available in ePub and PDF.

CW

We always like to see people being innovative.

Dear 2600:

For clarification on ideas not posted elsewhere, I have posted my work on several message boards and now have a 14-page Amazon Kindle book. I posted on message boards because I have needed to share my idea and receive input. I know from experience that posting a website or book is futile, because you must convince the reader there is reason to read your work. If you spam message boards, no one will respect your work. However, I think my book is suited to the *2600* readers. It is a way to make educated guesses at "p" in $N=p*q$.

The actual work has been posted, but perhaps new work such as the application of the math may be of interest to readers. Solving $N=p*q$ defeats the mathematical one-way-function RSA is based on. However, applying the math to real world keys and solving the private key, knowing only the public key and enciphered message, is another problem in itself.

The problem is valuable to study. That is why I think it would make a good challenge in *2600*. I, like every other reader, may have good ideas. But it is *2600* that provides the medium that allows good ideas and good projects to be recognized.

Yes, if we do find the solution, PGP would be rendered useless. Wait, I am only kidding, because my equations become more computational with an N in the millions of digits. But I ask you to look at my work and see if anyone finds it as interesting as the amount of work I put into it.

My book can be found at: www.amazon.com/Prime-Number-Factors-that-Solve-ebook/dp/B079XYZ596/. Download it once and read it on your Kindle device, PC, phones, or tablets. Use features like bookmarks, note taking, and highlighting.

Bobby Joe Snyder

We look forward to seeing what our readers think of all this.

Political Intrigue

Dear 2600:

I was pleased to read in *2600* 34:4 (Winter 2017-2018) that someone else didn't believe that "17 Intel agencies all agree" that the Russians hacked into the DNC computers ("The Russian Hacking Diatribe, and Why It Is Complete Agitprop Nonsense (And, No, I'm not a Trump Supporter)" by Doc Slow). When I first heard the talking point on TV news "all 17 intelligence agencies agree," my first reaction was to ask the talking head to *name* all 17 agencies. Had the talking head known the names of all the agencies, they never would have made such a stupid statement. They would (should) have known that all 17 could never have been involved in such a domestic investigation.

I spent four years working for one of those agencies and, by law, we were prohibited from assisting in civilian police matters. So, of the so-called 17 agencies, these four agencies could not have possibly examined the Democratic National Committee (DNC) server and concluded that the Russians had hacked it:

1. Air Force Intelligence
2. Army Intelligence
3. Marine Corps Intelligence
4. Navy Intelligence

The Posse Comitatus Act of June 18, 1878 prohibits the federal government from using federal military personnel to enforce domestic policies within the United States. While the act originally applied only to the Army, it was later amended to include the Air Force - and the Department of the Navy has regulations that effectively prohibit them as well.

The DNC is a private civilian organization. There is no way that any military intelligence agency can legally investigate a private U.S. company directly or indirectly by assisting local or federal police. That is against the law. When I served in an Army intelligence unit, everyone knew that we could not assist with domestic police matters.

The narrative that all 17 intel agencies agreed that the Russians had hacked the DNC server soon fell apart and on 29 June 2017, *The New York Times* issued a correction to the Maggie Haberman story and admitted that there were only four of 17 agencies that had actually reviewed the findings of the third party report.

The assessment was actually made by four intelligence agencies: the Office of the Director of National Intelligence, the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency. Note that none of these agencies ever had access to the actual breached server.

The lie that all 17 intel agencies agreed that the Russians were responsible for the DNC breach was started by the Director of National Intelligence, James Clapper, during his testimony before the Senate Judiciary Committee. This is at least the second time that Clapper has now been proven to have committed perjury under oath.

It is interesting that the DNC *refused* to allow the FBI to access their servers. Director Comey testified to this under oath. None of the intel agencies ever had access to the original DNC servers that were breached. None.

The DNC hired Crowdstrike to investigate the breach and Crowdstrike issued a written report that four intel agencies read and agreed with. Does this seem strange to anyone?

At some point, the FBI was given a reconstructed server image by Crowdstrike, but the FBI never examined the actual hacked server. In fact, the DNC destroyed the compromised servers. What was on the DNC server that the DNC did not want the FBI to see? Why were they destroyed? What were they hiding?

I encourage everyone to do their own research and reach their own conclusions. I for one have not found any conclusive evidence that the DNC servers were breached by the Russian government agencies (GRU or FSB). Guccifer 2.0 claims to have executed the breach, yet there is no proof given that he/she *didn't* do it. What bothers me the most is that Crowdstrike was paid for by the DNC and the FBI accepts as gospel their report. There has been no independent corroboration of Crowdstrike's claims.

David S. Lightman

We're not going to take up time and space debating or correcting points - as you say, people can do their own research. But there are certain things you must always keep in mind. People in power lie. They lie all the time. They do this to cover up all of the evil crap they're involved in. You may be able to say that you've found no evidence of Russian collusion, but we think it would be pretty amazing if you had that level of access and were keeping us in the loop. If you do, please send us some actual documentation - it won't go to waste, we promise. What we see far too often are people who accurately point to the lies coming from the camps of their political opponents who are then somehow completely blind to those coming from the people they like. This blindness is what is so dangerous and it's what leads to regimes where future historians wonder how people ever allowed certain things to happen.

Dear 2600:

Re Doc Slow's article on Russian election hacking (34:4), challenging the assertions made in the USIC JAR Grizzly Steppe report that Russia hacked the DNC: The report states that the malware was developed in a Russian language environment and was compiled in a time zone with major Russian cities. No doubt these could be faked and are not conclusive on their own. However, the JAR only contains unclassified information and does not include additional publicly available evidence such as:

- Dutch intelligence service (AIVD) penetrated the Russian operation and watched while the DNC hack occurred and took photos of the perpetrators via compromised webcams
- Trump Tower meeting where Russian agents offered hacked emails
- Similar Russian operations have targeted prominent Russia critics and European political candidates not sympathetic to Moscow
- Guccifer 2.0 has been proven to be a member of Russian Military Intelligence (GRU)

It is crucial to understand we are a target of a new form of warfare. The public's mind is the battlefield, and our political beliefs are exaggerated and used against us. Skepticism of government and those in power is crucial, but this skepticism has been weaponized via numerous methods. One method is the utilization of fake "whistleblowers" aka Russian intelligence assets: Assange,

Snowden, and Manning. Their purpose is to undermine the intelligence agencies that pose the greatest threat to Russia and its attempts to spread authoritarianism worldwide. Our future depends on us not falling for the lie.

Hannibal

While leaks may have benefited Russian intelligence, it's quite unfair to define those revealing the truth as assets of Russia. The leaks also benefit those who want to learn the facts. If anything, the absence of leaks from all sides is what was most detrimental.

Dear 2600:

Regarding 34:4, it never occurred to me to write and tell you that you are doing a fine service covering the Trump fiasco any more than write to tell you what a great job on all the other subjects you cover. Why would I? I assumed that 99 percent of your subscribers would agree with you, and with me.

I tend to think of Trump supporters as brain dead red-necks, though I have friends who do not fit that description. You probably have a lot of security professionals and well-off IT folks who typically vote Republican, no matter what. I recognize that intellectually; it's just that I can't see why it isn't support while holding their noses, as was mine for Hillary.

The obvious abuse of this administration of the law, human rights, and hackers in particular needs to be addressed wherever possible. Which is still possible here. And won't be if they have their way. I'm hoping the general incompetence they have demonstrated in getting legislation passed will allow this cycle to pass as shameful memory, but in any case, please keep up the good work.

I suspect, and hope, the volume of mail you receive on this topic does not reflect the general beliefs of your readers. One way to tell is to see how they vote with their wallets. How are subscriptions and sales doing?

OWA

Well, we're still here, so that tells us there's enough support and that we know how to stretch a buck. What we try to remember - and what we've always known to some degree - is that things are never as simple as they seem and that solutions aren't implemented overnight. It's a mistake to assume that your opponents are idiots because you'll often be disappointed and consequently outwitted. It's also a mistake to write off potential allies due to inevitable differences in opinion on one issue or another. Unification is key in order to achieve a desired effect.

Dear 2600:

Stormy Daniels is also on the Google Blacklist.

C F M

At press time, this was mostly true. Unlike most other celebrities, this name doesn't display "suggest results" on a Google search bar using Google Instant. Oddly, the name will complete with other names and words appended, such as "stormy daniels anderson cooper" and others. You can view our original expose on this back in 2010 at www.2600.com/googleblacklist/. We don't have the time to keep the list updated, but are happy to provide interesting updates like this one when they come in.

Contributors

Dear 2600:

I hope you are reading this. I live in a suburb of Chicago. This is not important, but I had some bad luck and ended up with a disability. It's not important as I'm someone with no hacking skills. But I have been read-

ing your magazine for about five years. I love the stuff I understand and I'm trying to learn what I don't fully understand.

If you are open to this offer, I would love to be part of the 2600 world. If you want or could do this, I would love to go through all the emails you don't have time to read. Just forward to me. With that in mind, like I said, no hacking skills but I can figure out what looks important or would be a waste of your time. I can then make a summary of the good questions you may want to consider.

I am not looking for money. I am looking to be involved with something like this. The only cost - and not even a cost - I would love the lifetime offer you just had on the radio even though this sounds like a deal of a lifetime. Unfortunately, on disability money is very tight but free time is plenty.

Mike

And you say you have no hacking skills! That was a really good social engineering attempt there, trying to get us to send you private mail. Well done, but we've been around the block a few times. We do sympathize with your plight, as many of us are quite familiar with similar circumstances. The best thing you can do to contribute is to write! That is how you can get a subscription among other things. And don't tell us you have nothing to contribute because you have no skills. Everyone who has even a fleeting interest in the hacker world has had some kind of experience that's unique to them and relevant to the hacker community. And everyone is likely to have more. Share these and we will share what we have. The lifetime digital digest offer you referred to isn't part of this, at least not yet. We're certain it will be at some point in some fashion.

Dear 2600:

My screen reader/web browser (Internet Explorer 11) has been having some difficulties accessing the magazine link on your website. When the link is clicked, the home page is still displayed.

I used to read the magazine a long time ago. I would like to submit an article for publication. Please can you tell me if the email address is still articles@2600.com? Do you have any other requirements besides it being in plain text?

Nigel

While we prefer plain text, we will endeavor to read other formats. The only real requirement is that you write about something you're enthused by and apply a hacker mindset to it. If you're familiar with our magazine, you already know what that's like.

We haven't heard about the issues you experienced trying to access our site, nor have we been able to replicate them. We'll follow up if others report similar results.

Dear 2600:

Would an article about how scientists regularly hack equipment, software, and otherwise repurpose materials to run experiments be of interest? I've had many experiences as a research student where I've used secondhand equipment that was originally built for one purpose (such as having a piece designed for use with high-pressure gases and repurposing it to work with slow-flow liquids) or designing custom parts to work with existing equipment as there weren't any on the market.

TaN

Anything that involves hacking equipment or software is by default of interest to us and our readers. We

will be camped out by our mailbox awaiting your article.

Donors

Dear 2600:

I am an instructor at Sauk Valley Community College and have recently taken over sponsorship of our college's tech club. I would like to request a free subscription to 2600. We are looking to reinvigorate the club with interesting projects for the student members to try as a group and on their own. Having a subscription would be greatly beneficial! The club has little funding for purchases due to lackluster sponsorship in the past, which we are working to correct, but we hope to be able to receive a complimentary subscription to 2600 for a while until things improve.

Can this email be forwarded to whoever would be in charge of approving such requests?

Thank you so much in advance. I know the students will get so much from the subscription, especially a renewed sense of interest and curiosity.

V

As luck would have it, we had a spare lifetime subscription lying around which we were able to donate to this fine institution. Don't thank us - thank the kind subscriber who decided to go digital and donate their existing paper subscription to someone like you. For those of you interested in making such a donation, simply go to the "Lifetime Subscription Digital Upgrade" section of store.2600.com and ask to have your remaining lifetime paper issues donated. Needless to say, we keep all of this anonymous.

Meeting News

Dear 2600:

Thanks for the Buenos Aires meeting point upgrade! Over the years, we have moved it many times in order to find a better place, with accessible prices and comfortable facilities for a 2600 meeting. In a very big city like Buenos Aires, it is very difficult to find a place that is accessible to all the participants who live far away from each other. I tell you that there are also in Argentina many other not-official-2600-meetings running every month in La Plata (I heard from them several years ago), Resistencia (in the last issue there was a request to make it official), Parana (they are waiting to make it stable to convert it to be official), and maybe even more. In case you find so much hacker activity strange, know that we drink mate all the day!.

Pablo

This is really heartening to hear. Thanks for the updates. Our biggest concern is how small we can possibly make the type on our printed meeting page if all of these new meetings are added.

Dear 2600:

I'm trying to start a SecTalk in Holland. Could you please connect me to the Utrecht 2600 guys? Maybe we can exchange info and work together on it.

A.K.

We don't give out private info, but hopefully they will read about it here and figure out how to track you down. Or you can just show up at their monthly meeting, which is exactly where such things are discussed. In cases like this, it's really handy to have a website up so people can make personal contact. We just can't give out that info, nor do we have the time to act as a conduit.

Dear 2600:

Who set up the Youngstown, Ohio meeting? I'm at Panera for the first time and there is no one here.

Jamey

This has been a problem at meetings everywhere since they began. New people show up and can't find other people. Sometimes people show up later and sometimes the newcomers give up before that happens. Other times, nobody shows up for one reason or another. This is why we try to make it simple by having a constant day that's easy to remember (first Friday), occurring infrequently enough (monthly) to make it more of a special event that's less likely to be missed. When we get too many such reports without hearing actual updates from the meetings in question either through email or their own websites, those meetings will likely get delisted. The opportunity always exists to restart or reorganize a meeting in a particular place.

Dear 2600:

Hi. I from kazakhstan. My name is Erman. Where is hacing

Super boy you

Anyone laughing at this should try and communicate with someone while only speaking Kazakh. Fortunately, we now have meetings in Kazakhstan so there's an actual answer to that question on our meetings page.

Dear 2600:

I would like to organize a meeting, I'm not sure if there will be interest, but I was miserable when I did not find my city and country on your list! Best regards and have a nice day.

**Sebastian
Wroclaw, Poland**

You can fix that misery by starting a meeting right there in Wroclaw. We think that's a great location. What's important is to make sure your meeting is in a publicly accessible place and that nobody is excluded. You can find more guidelines at www.2600.com/meetings/guidelines.html.

Dear 2600:

Hello fine folks! I am a refugee from America, living in a country full of beautiful women, great beer, and wide open spaces called Poland. There are no 2600 meetings here, but I love listening to *Off The Hook* and some of my Polish friends dig it too. Is there anywhere in Poland where I can buy the magazine? Can I subscribe and have it mailed to a friend's house in Warsaw? I would *much* prefer paper copies over digital. Thanks!

Ian

If you're in Warsaw, that's only a few hours away by train if you want to join forces with the previous writer and get a meeting going. As for subscribing, you can do that from anywhere. It's a royal pain to get retail store distribution overseas and it almost always winds up costing us money instead of the other way around. Subscriptions are comparatively simple, assuming you have reliable mail service. Simply go to store.2600.com for easy options that will have issues coming your way in no time.

Dear 2600:

We've established a regular group for the Campaign-Urbana 2600 and are passing off our twitter handle: @cu2600. In the future, we may be changing meeting venues. If/when that happens, should we just email meetings@2600.com to update the 2600 meetings list?

Steve

That is the standard way of updating your location, as-

suming you have a history of sending us updates or have your own website that also reflects the change. We cannot advise strongly enough that changing locations should be kept to a minimum, as new people will continue to show up at the old place since they may be looking at an old issue or otherwise haven't gotten the word yet. This is why it's especially important when starting a new meeting to make sure the location you choose is a good one. It's also wise for new meetings to run for a while before submitting their info to us to ensure that the location works, even if it's only with a couple of people testing the waters.

Dear 2600:

Hey! I tried to join the local meeting in Austria today, but I experienced problems. The Cafe mentioned on the meetings page does not exist anymore (Cafe Haltestelle) and I also didn't find any group of people.

So I am wondering if this meeting is still up?

Framework Conceptions

It does appear to be closed so, not having heard from anyone who's part of this meeting, we regrettably must delist it, effective immediately. Please let us know if you start up a new one by emailing meetings@2600.com.

Dear 2600:

I just moved to Boise, Idaho from San Diego, California. I figured I'd drop by the 2600 meeting in Boise last night, but it appears that nobody was running one even though the website has a 2600 meeting posted for Boise. I was an active member of the San Diego and Fort Lauderdale 2600 meetings. Anyway, figured I'd reach out to you all to see if you could put me in touch with whoever typically hosts the meetings in Boise. I want to confirm whether or not it's an active meeting. If not, I'd like to start one up here in Boise. I already host a weekly meetup on Meetup.com. To view the page, you can go to boise-hackers.com and it'll redirect you to the Meetup page.

Brent

At this point, we'd say it's safe for you to help reorganize this meeting as we're not showing any updates from Boise for a while. Plus, you clearly have experience with previous successful meetings. Just follow the guidelines on our page (www.2600.com/meetings) and keep us updated. Good luck!

Dear 2600:

Seen Asmodeus' post on latest magazine about holding a meetup in Cardiff or Newport in Wales.

Any way of getting in touch as I've also considered it but need a delegate to start this.

Andi

The helpful info will be in the third paragraph. The second paragraph will be devoted to the impressive amount of language differences that seem to pop up in these discussions and the first paragraph (this one) exists to explain all of this.

We're a paper magazine, so the word "post" is unusual when referring to a letter, but it also harkens back to the days of "posting a letter," so it's kind of a circular evolution. And we call them meetings, not meetups, as we have nothing to do with the social networking business and certainly don't need it in order to have people gather in various places. A delegate? For one of our meetings? It all sounds so intriguing now. We would have said "contact," which, in retrospect, sounds more like a criminal conspiracy.

To answer your question, we don't give out personal info, but there's a good chance the other person will see

this and you both will become aware that there's more than one person wanting to make this happen. We will help publicize the first meeting location that we're given and it should grow from there.

Dear 2600:

I'd like to get our meeting (Lexington, Virginia) listed. We've been running it since January and have had three or more people at every meeting. We meet at the Lexington Collaboratory.

We've got a very simple web page up at www.rock-bridge2600.com (it's intentionally very plain) with contact info and location. I am usually idling in #va2600 on irc.2600.net (talked about it with the other 2600s there (Charlottesville and NoVA) and they're fine with that).

Our last meeting was attended by six people, one brand-new attendee who's been reading *2600 Magazine* for over 20 years! We'd like to get listed on the site and in the magazine directory.

glitch

Consider it done. Please let us know how the meetings go.

Dear 2600:

The New Jersey meeting is still going strong. We're still meeting every month at the Dragonfly Cafe. Recently, there was a small group, but the proprietor said some people came and left when seeing no one was there at precisely five o'clock. You might want to remind readers to hang out a while since people come and go throughout the evening.

Ray

This is a good rule of thumb for any meeting. Too often, people give up quickly when they don't see other people. Of course, hanging out by yourself for an extended period of time isn't always the most comfortable thing. That's why it's always good to have at least one person around who knows what's going on throughout the entire meeting period.

The Hacker Spirit

Dear 2600:

Hello, I am an "inventor."

I have listened to your WBAI radio station show for years. I subscribe to *2600* and hope to have time this summer to engulf every issue in earnest. I met a few of you at the most recent New York City Maker Faire. I am currently taking two classes at Mohawk Valley Community College. One is an online honor's research class. The other is a materials engineering class.

I am having some "issues" with the online honor's research class which I believe the "hacker community" can help me with.

I have attached email messages which provide background on the whole story. In short, the professor is using Blackboard to restrict my postings to course folders and discussion folders, not allowing for either "late" or "early" submissions. As weekly postings are required for the course, I would like to have access to these folders whenever I want. (It probably would be best if I could insert time and dates which apply to the week in the semester for which the assignment was or will be due.)

I am a "crammer" and fully expect to complete the work for the course by the end of the semester in accordance with my "learning style." We are now at week seven of a 15-week course. This rigid "week by week"

required posting consistency - which has been demanded by the professor - does not work for me. I move by inspiration. Usually, a productive "spurt" will come to me; I do the work during that time. Then it is done.

This "step wise" approach to learning is beyond boring, and I will have vacations and trips to go to for which I do not plan to even be thinking about this class. I want to get it all done, soon. Posted, and hopefully indelibly recorded for all to see, with the appropriate dates marked.

Are there any known "hacks" to Blackboard which I may utilize in order to fulfill this aim? I have already discovered a back door to the discussions folder on the course Blackboard site. I had posted my "reflective writings" there in advance - which the professor has objected to. She has already informed me that the most that I can expect is a "B" grade for not having posted assignment "reflective writings" and "discussion threads and replies to classmate comments" previously. She now threatens to give me zeros for the postings which I have already made for the future weeks of the class.

I have discussed the matter with school administrators who inform me that the professor can impose whatever policies she chooses regarding the learning outcomes and procedures for the class. They say that she can penalize me for having posted my school work late or in advance, and have encouraged me to either drop the course and take it again in the fall (thereby losing the money that I paid for tuition). My other option would be to stay in the online course and comply with the professor's dictates by following her weekly time schedule. If she does impose penalties for my already having posted work to future week discussion folders - and I expect that she will - I can look forward to a grade of "C" at best.

What to do? I think those in the hacker and maker communities might provide me with a number of strategies and suggestions. Hacking Blackboard to suit my aims and learning style seems to be an obvious place to start.

I have provided all necessary emails and links for your perusal....

I pledge to write an article for *2600 Magazine* regarding the outcome of this online Blackboard course experience when all is said and done.

Thanking you all - in advance.

N

Thanks for sharing all of this - and there really was quite a lot of it. Everything from the aforementioned conflicts with an online professor, your plans to build a zeppelin, some poems, and even your full login credentials for your Blackboard account (which we are ignoring). We appreciate and admire your passion.

Here's the thing, though. What you're learning here is the rigid and uncompromising atmosphere that tends to prevail in American schools, both on the grade level and in college. Free thinkers are often the enemy and are seen as a threat. While we would never advise anyone to simply accept this, we are kind of surprised that this seems new to you. We get letters from kids in grade school who are fed up with this kind of crap. It's something the hacker world is quite familiar with: curriculums that move too slowly or focus on the wrong things. But there's precious little that can be done to make the people running things change, other than to let as many people as possible know about it. That is how change comes about.

We do find it amusing that even online courses fall into this trap, and to face such discipline without even having to show up in person is a true sign of our times. But maybe this is how you can benefit. If you're able to see ahead and complete the assignments in advance, there's no reason on earth you shouldn't continue to do that. But make them think you're playing by the rules by not actually posting these assignments until the moment they're due. Perhaps you can even write a script to do this for you. The biggest hack of all would be to have these dimwits convinced that you're a model student who's following all the rules when in actuality you're doing everything the way you want to and just not letting them in on it. There are few better feelings. (Of course, this won't help if your assignments are late, but we can't really think of anything short of a time machine that would.)

We know that for many, it's easy to dismiss people who insist on not following the rules and we're certain to get letters that tell us why we should be doing that right now. At some point you have to ask yourself why it's so important to do things in one particular way just because someone tells you to. Is there any actual harm in trying something else or in asking a whole bunch of questions? This is, after all, what hackers do.

Dear 2600:

Are you looking for the community to send articles into the magazine? I would love to write an article for 2600.

Jim

We absolutely are looking for precisely that. In fact, without the hacker community, we don't exist. Every last one of us has a unique perspective on something, and tying that into the hacker mentality is what we're all about. So please, find something that interests you, apply some hacker observations and ingenuity to it, and piece your words together. You'll be glad you did.

Dear 2600:

Thanks for publishing my article on smart watches in 34:4. It's good to know that I'm still worthy of being published in The Mag. I'm attending a local computer security group in my current hometown of Orlando, and I'll be distributing copies of the Booklet I created from the article (<http://CheshireCatalyst.Com/SmartWatch.pdf>). You can just fold the printout in half, and then in half again to make a booklet. I used Publisher in Greeting Card format to create it. When I publish multiple copies, I print out two copies, then put one in the input hopper turned 180 degrees from the one below it, and tell the copier to print 1-2 (input one page, but print it on two sides of the paper. This gives me two copies of the booklet on one sheet that I can cut in half to give me two copies of the booklet. I'll print out 20 copies to give me 40 booklets to hand out at the meeting.

**Richard Cheshire
Phreak & Hacker**

We would have sent you issues, you know. But this is also an ingenious way of getting the word out.

Dear 2600:

mashable.com has class on how to hack. White Hat jobs opening thanks

sasse

You're not describing hacking, not even a little. No website is going to teach you how to hack. And if you even use the phrase "white hat," you've got your foot

mostly planted in the corporate world. Also, we're not Twitter, so full sentences are welcome.

Drama

Dear 2600:

It started with a picture of a payphone....

In the late Summer of 2017, I began going to a chiropractor near my house. A friend of mine from high school was recently depressed, so I decided to take a picture of a phone at an abandoned gas station near the chiropractor's office to show it to him to remind him of the good times. I would go to look at that payphone and think of him often. However, the payphone and abandoned gas station were near a child day care center. I got the sense that they probably didn't want me around, so I stopped going there. After that, the cops started showing up around the shopping plaza often but soon disappeared.

Several months later near Halloween, I put up an ad for a dominatrix on Craigslist. That weekend I went to a Meetup group I go to often and a friend there (who I'll call Joe) said he had a rough day. Somebody had mentioned drama and had said that we had drama within the group, but it was "behind the scenes" and, in saying so, he gave me a knowing look.

At the restaurant, I sent Joe a text saying "So, can I tell you what happened?" He responded with a text: "I'm going to head over to the bowling alley now we can talk then or if you want to call me when you're heading over." So I go to the bowling alley and Joe starts to deny that anything happened. Joe also tells me that "The cops aren't tracking your phone." I knew I was being spied on, but they went to the trouble to call my friend up and tell him to deny anything happened.

A few months later near New Year's Eve I met a girl and we exchanged numbers and began talking and texting. At some point in the conversation, she notices that all my calls and texts say "Remote" and it is only for my number. She asks if I'm hacking her phone. I play it off, and fortunately she believes me. So here is a second time I catch law enforcement spying on me.

And finally, three weeks ago, I get the flu for about two weeks and I send some texts saying that I'm feeling really down. When I finally got back to the chiropractor, I see the cops waiting for me as I drive up. After three weeks in a row of the cops waiting for me, I had enough of this and decide to go to another chiropractor.

If I had been sending angry, violent texts, I would understand this behavior, but in fact my phone activity has been just the opposite. I repeatedly talk about non-violence (having some kinky fun with a dominatrix isn't real violence in my book), I have texts where I talk about getting \$200 out of an ATM and give it to every homeless person I could find. I have texts where I talk about a food pantry I volunteer at (incidentally, I'm almost sure they contacted someone I know at the food pantry, can you believe that!). This is not some abstract threat of spying, this is straight out of 1984.

I can only summarize that the notion of nonviolence is philosophically incomprehensible to law enforcement agents. They have chosen violence as an acceptable means of conduct and are thus on a slippery slope that requires more and more intrusion into the lives of others for some perceived greater good, when in the end it is all for naught. Their fretting and violence can't stop the inevitable sickness, aging, and ultimately death that

victor

Dear 2600:

Thanks in advance.

Name Redacted

Visibility

Dear 2600:

I have at least three ready-to-use ideas for 2600.com, too. When do you have seven minutes to discuss whether these are good fit for you?

Kata Gazso
CRO Specialist Executive

Dear 2600:

Bruce

[illegible]

Dear 2600:

When is the best time for you to have a six or seven minute call to see whether it is something that 2600 Enterprises, Inc. can benefit from?

Kata Gazso

CRO Specialist Executive

You seem obsessed with us. Look at all the work you've done so far. This can't possibly be spam because it's so personalized. And automated spam would never make mistakes like saying Hackstory's store is easier to navigate than ours. We never heard of them and can't even find their store, let alone navigate it! But at least

you're willing to talk with us for only six minutes now. We'll see what we can do.

Dear 2600:

We plan to screen documentaries about the history of hacking and *Freedom Downtime* would be a very interesting choice for us.

Would you grant us permission to screen your movie? And what would be your terms for such a screening during a noncommercial event?

I remain at your disposal should you require any additional question or information.

JG

You can still get a double DVD copy of our documentary at store.2600.com (assuming you're able to navigate it without the confusion the previous writer had). Anyone can screen it anywhere at any time. Those are our terms and we won't change them for anyone.

Dear 2600:

You used to have a list of places where you could buy 2600 at a regular brick and mortar store, but I can't find it. Can it only be bought digitally or ordered directly from your site? I was hoping to find a place in Sweden or Norway to buy a copy.

Dokter

This remains a topic of frustration for us as well. It's likely you won't be able to find a copy in a store overseas, since it's incredibly difficult and expensive to be carried there. On those occasions where we've managed to do this, we either wind up not getting paid or actually owing money due to the poor terms we get. As for a listing of places in the United States and Canada, this is something our distributors need to share with us so we can share it with you. In many cases, this information is treated as a trade secret that we're not allowed to have. We'll keep trying to get a comprehensive list. We can say with certainty that we're carried in every Barnes and Noble store in the United States and, last we checked, Chapters in Canada. We are open to supplying any store domestically that expresses an interest.

Dear 2600:

2600.com confused me. I was looking for sites providing/selling event tickets and bumped into yours, too. I clicked but your user journey confused me as it does with others, too, based on SimilarWeb.

Not only me, but 36.58 percent of your visitors leave less than 0:01:08 seconds and go to hackstory.net. This must cost you a lot of money if you put lots of efforts into creating content or paying for ads. We have a few brilliant ideas to stop this madness that has worked with 5967 other sites, like Hackstory or phx2600.org, too.

Kata Gazso

CRO Specialist Executive

Well, now you're just talking shit. You expect us to believe you were "confused" by our website, so you went to a completely different site that doesn't even offer what you claim to be looking for? Are we supposed to be frustrated by the appearance of "hack" and "2600" in these other sites, one of which is an outlet for our own monthly meetings?

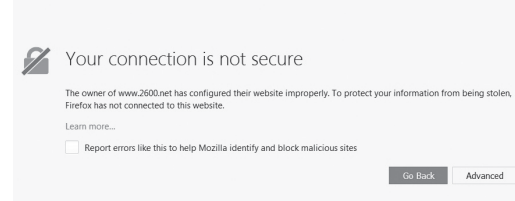
You may fool countless companies and others on the net with your overly specific and fake personal contact, spam following up on spam, etc. You are on notice. Of course, you are also a machine. If you persist, you will be a stressed out machine. Hoping to never hear from you again. But, of course, we all know that's just wishful thinking.

Summer 2018

Dear 2600:

I received the message "Your connection is not secure" when going to your site. Why? (The image is attached.)

Albert



Every subdomain of every domain requires an SSL certificate in order to be deemed "secure" and there just aren't enough hours in the day to cover all the ones we have, considering certificates are constantly expiring and being renewed. You're using one (www.2600.net) that we don't publicize. You will have a secure connection to the exact same site by using www.2600.com or 2600.com.

Dear 2600:

I just wanted to give you a quick update on the availability of the latest issue in my area.

I've been checking the Barnes and Noble in Plymouth Meeting, Pennsylvania for a number of weeks now. As of today at 2:30 pm, they still did not have the Spring issue in stock. They are displaying the Winter issue instead.

I also have been checking my local Micro Center in St. Davids/Villanova and they also do not have the latest issue available. They usually lag behind the local Barnes and Noble, but they should have it by now. They are also displaying the Winter issue.

I will check back with them both in a week or two. I hope they can work out the kinks in getting your magazine to the shelves.

Keep up the great work! I can't wait to read the Spring issue.

LC

Unfortunately, a number of people had to wait for the Spring issue, as there were major problems with new shipping methods being used by certain stores along with our distributor, resulting in up to a month of lost sales for us. This kind of thing is incredibly frustrating as we're powerless to do anything about it.

Dear 2600:

I cut to the chase: SimilarWeb says that 36.58 percent of your visitors jump over to sites like Hackstory and spend their money there instead. I can show you 30+ of case studies of sites like phx2600.org how we stopped such exodus and retained at least 57 percent more visitors on their Shopify store and turned them into buyers.

I wanted to discuss in a seven minute Skype call whether it is something that 2600 Enterprises, Inc. can benefit from, but first, you probably want to check "how" you can lift your sales. So just click here to learn more: www.optimonk.com/shopify-stores.

Talk soon.

Kata Gazso

CRO Specialist Executive

Email: kata.gazso@optimonk.com

Tel: +1 415 800 4445

You might be talking soon, but not to us. We suspect you will shortly be getting quite a few calls from people who are curious about your services and business practices.

Page 41

The amount of unsolicited mail we keep getting from you is staggering, and all of it is "personalized" to make it seem like you actually know something about us or the other sites you claim to be working with. As technology keeps improving, it becomes more and more difficult to tell when you're dealing with humans or with algorithms. But there are always warning signs. In this case, there were several. Why would these people be emailing our letters department to help improve our sales? Why did they refer to other companies who aren't competing with us in any way, but have names that might make it appear as if they do? Why the repeated emails at a rate no sane human could keep up with?

If we didn't have experience in the field - or had received a whole lot less email - we might have been fooled into responding and being pressured into buying something we had no need for. The sad fact is that people are taken in by this sort of thing all the time, some far worse than others. And soon, you won't even be able to tell if you're actually speaking with a human on the phone. That means we can count on seeing more sophisticated spam attempts in the future. It also means we can count on people believing we're also computers on the phone when we're not. Fun times ahead.

Dear 2600:

It is my great pleasure to confirm to you that new dates for Sudan Poultry Expo, 10th Session will be on 20th to 23rd February 2019, at Khartoum International Fair Ground and on schedule. SPE is a major specialized event dedicated to development of poultry, livestock, and agricultural production in Sudan and Africa, with animal number exceeding 140 million cattle, one of the largest in Africa and the Middle East.

Osama Mustafa

We'll spare you the rest of this lengthy email, which went into great detail about what we can expect at this poultry expo. (It's actually gotten a number of us enthused enough to consider going.) This is the kind of spam we truly don't understand. There's no link, offer, or request for money - just info on an event we've never expressed any interest in and which is about as far removed from anything we do as we could imagine. And now we feel as if we're somehow a part of it.

Dear 2600:

This is sort of an "off" question, but what's your take on a private company branding themselves as "2600 Security?" Specifically, the website 2600.dk used to represent the Danish hacker community, but the domain has since been sold. The new ownership claimed to want to re-launch the site as a hacker community, but now appears to be launching a private security firm with a registered business under the "2600 Security" moniker. I'm sure there's no legal recourse or even a need for it, but what's your take on people using the name/brand?

Curious

It's misleading at best. There's not a whole lot more we can say, other than to point to this as a reason why you should never let domain names expire.

Being Alert

Dear 2600:

Yesterday my computer was hacked by a Microsoft alert from Windows regarding a virus alert and I was asked to call 1-833-886-5888 and to not turn off my computer, which is on an Internet, TV, and landline service

that I recently purchased from Optimum, a subsidiary of Altice USA, Inc.

Frankly speaking, I am a veteran (U.S. Army) and senior citizen, as old as Pope Francis (aged 81), and grew up as an "analog person" and not a "digital person" who is computer literate. However, I still have the intellectual curiosity to purchase your very meaningful and worthwhile magazine at Barnes and Noble where I am a "member."

The article by Doc Slow ("Russian Diatribe") caught my attention because he mentions Microsoft operating systems from which some "hackers" who say they are from Microsoft actually hacked my computer and wanted me to pay a fee to unlock this virus which they actually alerted me to and told me not to turn off my computer and immediately call 1-833-886-5888. Frankly, I recognized that this was a con job and turned off my computer and refused to follow up on any of their computer crisis baloney and I somehow got my computer up and running, as you can surmise from the fact that I am writing you this email, incidentally with no customer service from Optimum/Altice nor without having to pay the supposed representatives of Microsoft/Windows for their unwanted/expensive answers to the virus hacking my computer.

Your author specifically mentions that Microsoft is the most insecure OS (I hate initials, but I believe he means Operating System) and that it is specifically targeted by malware authors, state-sponsored or otherwise... etc., etc.

I wish your magazine continued success and even though I do not fully understand what the heck is going on in the new 21st century digital world of hackers and leakers, I have had my Chase/JPMorgan bank account hacked twice and Chase has had my Chase account number changed twice, both last year and this year in order to stop the pilfering of my bank accounts by very clever "malicious hackers" who utilized PayPal, etc. to steal money out of my Chase accounts.... However, I am happy to report that Chase/JPMorgan, after investigating my complaint, made full restoration to my account of the hacked/stolen money (more than one thousand dollars). They take a little amount at first and, once they get hooked in, they increase the amounts they steal from small amounts to larger amounts. All bank customers should be alerted to the fact that they should review their bank statements on a monthly basis, line-item by line-item, to make sure that the electronic withdrawals are correct. You have to review your bank statements very carefully and do a forensic financial accounting to make certain you're not being pilfered or robbed out of your money!

Frankly, I believe that hackers who only speak "digital" should learn to accommodate senior citizens/veterans with more "analog" words and language because most seniors simply do not comprehend or understand the "digital world of words" of this new and complicated new age.

Esteban

First off, congratulations on triumphing over the potential fraud you've been subjected to. Simply by paying attention and recognizing when something didn't quite seem right, you were able to save yourself considerable expense and inconvenience. So many people can learn from this example.

The divide between those who create, understand,

and prosper in today's digital world and those who feel left behind is not insignificant. It should never be minimized, mocked, or ignored. Everyone lives in a world with their own self-defined borders and those who choose to embrace other elements of life that don't necessarily include the latest developments in technology are no less worthy of its benefits - and certainly no less intelligent than those heavily into these technologies. After all, what good is the technology if it only works for a select few, or even a select many? We need to develop fail-safes and methods of protecting those who, for whatever reason, are unable to protect themselves. Your words serve as a bridge between these worlds and that is a true talent. We need more such voices and the rest of us need to listen and engage them more frequently.

The phone number that showed up on your computer is well documented as a scam. It has nothing to do with Microsoft. The fact that the fake alert showed up in the first place on your computer tells us that you might have had malware of some sort on your system. You need to run a full scan using a legitimate malware detector (Avast, AVG, Norton, etc.) and remove it. It's also possible that you have no malware and that this was simply a programming trick originating from a web page, making it look like you were infected when you were not. Either way, the scam involves giving the people at that phone number access to your machine so they can install truly malicious software and cause real damage, leaving you with no choice but to pay them. You may also get a phone call from someone claiming to be from Microsoft or equivalent wanting to "help" you with your system. This is always a scam, so never give people you don't personally know this kind of access. Instead, try to waste their time by telling them you have a Mac or something.

Your instincts have served you well. Don't ever think you're not computer literate because your actions and observations show that you can hold your own in cyberspace.

Dear 2600:

As Fry from *Futurama* says, "Not sure if 2600's messing with me or if it's just a misprint..."

Dear Mr. (or Miss or Mrs.) The Prophet, I recently received the Spring 2018 issue of 2600. It's always a toss-up between which I read first, the "Telecom Informer" or the letters. This issue I planned to read "Telecom Informer" first, but alas, you were not there. There was a moment I thought you decided to end your tell-all. I checked the Communiques page and your residence was listed as page 13. To the page numbers I went... 5, 7, 9, 19, 21, 23, 25, 19, 21, 23, 25, 27... I never found page 13. I even checked the envelope. Of course, my first thought was printer error. The magazine always seem to have issues with the printer (remember the inky-thumbprints issue?). But then the little voice in my head said "it's a trap!" So I thought I'd write. Then I realized I never told you about my visit to Central Office. I looked around for you but didn't find you. Instead, I listened to a bank of drop switches and tried to imagine the hum from several banks filling an entire floor of the building. It was dazzling in my head. I puzzled over the geography of the letters in our local phone numbers. MAin and BRoadway seemed to be popular, but I decided mine would be YUkon. I also found my grandpa's address in the phone book at the phone booth. I considered calling, but he passed away some time ago. Anyway, I'm not sure if there is anything

that can be done about the oddity of my Spring 2018 issue. Any assistance you could provide would be greatly appreciated. I hope you have a fabulous quarter.

Emily

Whenever such a catastrophe occurs, we always like to get our hands on the issue in question so we can wave it in the faces of those responsible and act all self-righteous. In addition, we will send you a replacement and additional stuff for your trouble.

Dear 2600:

The Cloud Act which was signed into law on March 23rd of this year is another nightmare for privacy rights. The Cloud Act allows law enforcement from other countries to access communications of American citizens whether it's email and Internet content and/or telephone calls. In giving access to American citizens' form of communications to foreign entities, it's giving them power to maybe charge an individual from the United States for a specific crime that otherwise would probably be off limits. This opens up the floodgates to do so. American citizens have our own judicial process/procedure and allowing foreign entities the power to sweep up communications totally goes around this very judicial process/procedure which is in place to protect rights such as free speech and privacy among others, but now is at the mercy of countries who shouldn't be given direct access to an individual's communications from here. American citizens' protections are eroded by giving foreign powers access to communications and this piece of legislation should have never been introduced or signed. Hopefully at some point it will be repealed, but the odds of that happening are probably long. The Cloud Act is a huge mistake.

Bill Miller

We don't believe foreign entities should sweep up our communications nor have the ability to arrest us. But we also believe this when our country is the foreign entity, something our government seems to believe shouldn't apply. And as long as they decide they're in the right to do this, we can't in good conscience say any other country shouldn't have that same power. But none of this really has anything to do with the Cloud Act, which we agree is a big mistake. But it's not foreign governments that will be given access to our data - it's our own government once again, which will make agreements with foreign governments and bypass the Fourth Amendment since the data isn't on U.S. soil. Conversely, it's feared that the U.S. government would be overly helpful towards some of these foreign governments by providing them with data on their own citizens that happens to be stored on servers in the United States. Basically, citizens all over the world lose due to the extra power our own government feels they're entitled to.

Requests

Dear 2600:

I would like to thank the whole 2600 team who work hard to publish this beautiful magazine. It is out regularly, four times a year, every year. Hats off to you guys, the readers really enjoy it. On a different note, I would like you guys to promise that, forever and ever, the current paper format will be kept so long as a paper version is published. This is just in case you ever imagined (again or ever) any form of alternative, new way of stapling, or whatever. So please, do you promise?

I write to share the following idea: would you consider releasing an ISO image of the original *Freedom Downtime* DVD in the 2600 store, or offer some form of download of it? The goal here would be to help preserve (and share with the world) the original subtitles' tracks of that DVD. I remember that in the months prior to the film's release, I helped 2600 translate *Freedom Downtime*. I found that experience was a truly collaborative and international effort. How nice to have participated. I am thinking that the result of those efforts could be shared more widely, and where better than having *Freedom Downtime* hosted at 2600.com?

And for the readers actually curious to see *Freedom Downtime* and read subtitles translated in a non-English language: please, oh please, do *not* use the Tube's subtitles... they can only suck. I encourage anybody to find a copy of the DVD for the best, and the most varied, choice of subtitles.

Some Buddy

This is a great idea and we would love nothing more than to implement it. However, we would likely run into issues with music rights and copyright that we had clearance for when the film was released onto video media, but which would be different for a downloaded version. It's insane and unfair, but that's how the laws currently work. That said, we will not stand in the way of anyone who wishes to do this.

And yes, we will keep the current format for future printed editions, staples and all. Nobody ever really seemed to care about that with so much intensity.

Dear 2600:

I was on this page of your site - www.2600.com/hacked_pages/1999/11/www.es.anl.gov/index.html - when I noticed you have a link to Four11 (www.four11.com/) which it seems is now offline.

Perhaps you could replace this link with one to our company? I think this will be useful for your visitors because we have a people search and background check feature that is a good alternative to Four11.

Joseph

You don't really get the purpose of a hacked website archive, do you? It's not to replace defunct companies with existing ones; it's to show what a hacked website looked like when it was hacked! Nothing more. If we start changing the links and companies referenced, it's not going to be much of an archive, is it?

Nice try, though. And we might have even revealed the name of your company if you hadn't become a pest with multiple emails on this subject.

Responses

Dear 2600:

Here are some comments on "What Happens When WHOIS Data Is Made Public" by Victor in 34:4:

Victor suggested: you probably want "private." I do not think "private" should even be an option. Let's say all-about-frogs-dot-org [aaf] is "good people." Sadly, there are lots of not-so-good people who host websites. A public WHOIS helps me presume whether aaf is likely to be a safe harbor (assuming someone nefarious has not hacked aaf, the viewable registered persons are real, et cetera).

For what it's worth, I have more domains than the average individual who has one or a few. I get relatively little or no spam and I know how to use mail rules, whitelists, blacklists, et cetera. I avoid using spam filters because of too many false positives (bad) and too many false negatives (annoying). Somewhere in between Bashar al-Assad (evil war criminal) and Malala Yousafzai, I consider myself essentially a good person.

One of my current paid tasks is to vet business end users who desire access to a partner business website. For that, the tools I use include ip2config and domain tools. One of my main frustrations is "private" domains.

"Private" registration is much like that wall that the current POTUS wishes to build... it may keep out desperate good people looking for a better life; bad apples will find a way under, over, or around.

The real solution to spam is to seek out and block spammers from the Internet. There is a difference between spamming and marketing, so it's technologically possible to separate evil spammers from annoying marketers who act responsibly. Phone spam also can be solved technologically by preventing spoofing and enforcing do-not-call rules.

gerry

We see the value in both arguments. Privacy is a right that we all are entitled to. However, the whois function on the net is virtually useless now, whereas before it was a great means of knowing the trust level you should attach to a new domain that you were communicating with, either via email or through the web. One thing that is frequently forgotten: back in the days where every domain could be looked up to find out the owner, it was entirely possible to put in fake info. Oftentimes, that fake info was enough to answer the question as to whether a site was genuine or linked to some other entity, all without anyone's privacy being violated. Having the same "privacy guard" name show up in place of the registrant doesn't really answer the whois query. It does, however, give registrars the ability to sell yet another product and give the illusion of security. After all, you don't really think they will protect your privacy when the authorities come knocking, do you?

Dear 2600:

Super happy with the PDF quality of *The Hacker Digest*. 2600 has been a part of my life for many years, so I am so happy you have chosen to make available past issues.

Once my tax return comes, I will be purchasing all back issues and lifetime sub (digital as well).

I want to make these available to my two sons as they get older.... Can't thank you and your organization enough. Best of luck, always.

Alexander

This is the kind of feedback that really motivates us. As we slowly deplete our supply of the old back issues on paper, it's great to know that they will live on digitally. It's also been a really cool trip down Memory Lane for us, as we explore what was going on in every year of our existence, not to mention finally explaining what all those old covers meant.

Dear 2600:

Re: Historic Hacking (35:1) - it is true that FORTRAN is evil, so evil that nobody would have ever punched "for I = 1 to 10" on a card. Instead, it would have been something like "DO 3790 I = 1,10". This better

illustrates some of the true evility of FORTRAN. First, everything has to be in upper case. I remember helping a student who got a stream of error messages from a FORTRAN compiler. Everything looked fine on the printer that only did upper case, until I checked the source which was entirely in lower case (obviously not punched because punched cards only did upper case).

Even worse, the mysterious number "3790" would be the statement number of the CONTINUE statement at the end of the DO loop. If you duplicated a statement number, well, all bets were off. Your program would definitely fail, and it would take forever to find the cause in a large program with hundreds or thousands of line numbers. These line numbers were also frequently used with the even more evil GOTO statement, producing the famous spaghetti code so characteristic of FORTRAN.

Other subtle evilnesses of FORTRAN were the fact that the counter in a DO statement had to begin with the letters I, J, K, or L because all other variable names were implicitly floating point. And the loop could not start with 0, but had to start with 1 or higher (which leads to many off-by-one errors). And, finally, FORTRAN didn't care about spaces, so if you forgot the comma, the compiler would process it as DO3790I = 110, i.e., create a variable and assign it the value 110. Apparently a rocket once blew up because of this error.

No modern language has the concept of line numbers or goto statements. Well, not quite true. C does allow goto statements, but you must never use them (and C is not really modern either, but it still has some of its teeth). Basically, all the unique characteristics of FORTRAN are really, really bad ideas, quickly abandoned by all other language designers.

D1vr0c

And sometimes Memory Lane has its dark zones.

Dear 2600:

In Alexander Urbelis's article, he is completely incorrect and I hope he is not an attorney, as if he is he would starve.

While Russia did try and hack systems, the stolen info has been proved to be an inside job according to the DNC internal investigation, not a Russian hack.

Both Mueller and Clapper (former intelligence director) have stated repeatedly that no voting machine was ever hacked and no vote was ever changed. And due to the ignorance of the FBI not following the rules, the new judge in the Manafort/Gates cases has demanded all the info from the FBI or she will overturn this and void any confessions as well as throw this out with prejudice, meaning it can never be filed again by any attorney: local, state, or federal. Not surprisingly, the same thing is happening with Flynn and Papadopoulos as the FBI rushed in before they had all their ducks in a row and they then did not turn over all the information to the accused as they are required to do under law. In fact, they hid some back even after a motion of discovery was made. And that is not only illegal, it is a surefire way to get a case thrown out of court or a conviction overturned. And they have not learned anything as while they took everything from Trump's attorney Cohen, they again took everything! Under a warrant, they can only take what is related to Stormy Daniels and everything else they must return or violate a sacred pillar of U.S. law, and that is attorney-client privilege. Over 500 attorneys from both sides of the fence and the last six U.S. Attorney Generals have

all said the exact same thing. If the judge refuses to do this, she can be arrested and charged and brought before a judicial review and lose her license, which would end her career as a federal judge. And let's not even start to speak of what will happen to the prosecuting attorney in this instance as his punishment will be ten times worse.

And the major problem with Urbelis's myth is that on April 10th, Mueller told the *Washington Post* that there was "no evidence of collusion or obstruction" which effectively killed his investigation, as this is all he was allowed to investigate under his orders given to him when he was appointed and we also had members of the House and Senate Committees looking into this say the exact same thing. To investigate anything else violates the Special Counsel regulations and laws, which means nothing outside of this can be used in any way, shape, or form. As a person who works in a law firm, Urbelis should know that nothing that is not on a warrant can be taken or used, and nothing that is found or taken outside the scope of a strict and narrow designated investigation can be used.

Therefore, Donald Trump is the legitimate President of the United States and Urbelis should cease trying to overturn the 2016 elections. Not to mention that his article had no business being printed in your magazine. I and others read your magazine for the articles on hacking and new hacks and so on. We get enough talking head hogwash by just watching the nightly news; we don't need to get it here as well. It's your magazine, but if I am allowed to put in my two cents worth, I would from here on out refuse to print political stuff in the Alt 2600 magazine and let the tinfoil hat crowd on both sides of the political fence hash it out on the Internet and keep your magazine true to its agenda, dealing with hacks and electronics, not harebrained conspiracies from the politics. If they want that, they can watch CNN or MSNBC or the idiots on Comedy Central.

Daniel

We can't help but notice that you left out Fox News. Regardless, we're real sorry if you don't like the talking points that surround this article, but none of that was even addressed in it. The real topic had to do with operational security and the methods Robert Mueller is likely using for communications. A hacker perspective on that is extremely relevant, focusing on such topics as encryption, two-factor authentication vulnerabilities, zero-day exploits, and the dangers of being connected to the Internet. Quelling that discussion because the mere acknowledgment of an ongoing investigation might offend someone's political beliefs is not what we do. You may perceive a political bias when certain facts are referred to, but that doesn't make them any less factual. There were indictments, there were guilty pleas, and there is a continuing investigation. Stating facts is not an opinion.

And when precisely did we become known as the "Alt 2600 magazine?" You know you're writing to an actual magazine and not an old Usenet news group, right?

Dear 2600:

I just received a message about the message I sent to you. I haven't emailed you for two years, so if you have an inquiry from me, it's false.

Rocky

This happens now and then when someone's email address is forged, generating our auto-reply function and creating confusion like the above. We're sorry for that.

But why haven't you emailed us for two years?

EFFecting Digital Freedom

Grassroots Effort Kills Bad Computer Crime Bill in Georgia

by Jason Kelley

We didn't think we'd pull it off.

S.B. 315, a computer crime bill in Georgia, was introduced into the state's legislature in January. It passed the Georgia Senate in just over a month and the House shortly thereafter. S.B. 315 is one of many laws that have popped up over the last few decades which are modeled a bit on the Computer Fraud and Abuse Act, or CFAA, the infamous bill used to prosecute good-faith security researchers. But the Georgia bill would have done something totally new, and exceptionally dangerous.

Not only would the bill have created a new crime of "unauthorized computer access" in the state of Georgia - which is the country's third largest cybersecurity community - and have opened up independent researchers who identified vulnerabilities in computer systems to prosecution and sentencing of up to a year in jail, it would also have allowed for preemptive "active defense," giving authority under state law to companies to "hack back" or spy on potentially everyone from independent researchers to users whose devices have been compromised by malicious hackers. This precedent-setting legislation was, thankfully, vetoed at the very last minute by the state's governor.

But the bill's narrow defeat is an important lesson. How did something so widely criticized by the community sail so rapidly through the state's legislature? And how was it, in the end, defeated?

The bill began its life out of, apparently, embarrassment. In August 2016, security researcher Logan Lamb at the Oak Ridge National Lab in Tennessee had been searching Kennesaw State University's Center for Election Systems' website for public election information when he discovered sensitive documents that were openly available. "You could just go to the root of where they were hosting all the files and just download everything without logging in," Lamb told Politico, who broke the story.

He wrote a script to download and take a look at what exactly was available, and came back with data including registration records for the state's 6.7 million voters and lots of additional sensitive data that should never have been made public. Worse still, he discovered the site was using an old, seriously vulnerable version of Drupal as its back end, which allowed attackers to potentially take control of any site that used the software.

After accidentally discovering the various vulnerabilities and reporting them directly, Lamb was disappointed that the state hadn't taken his discoveries seriously. Georgia lawmakers responded to this, not with concern that the data had been left in the open, but rather, with anger that it wasn't illegal for Lamb to access that publicly accessible data - and thus Georgia's S.B. 315 was born. (As the state's attorney general's office said, they wanted to criminalize "poking around." And while we believe Lamb's actions would have been legal even had S.B. 315 become law, it's plausible that Georgia would have argued to the contrary.)

Did the bill have good intentions? Almost certainly. And this is why we must pay close attention to attempts to legislate computer and technology usage - without a deep understanding of how cybersecurity works, these good intentions are easily translated into fast-moving, wide-reaching legislation. From its introduction until the date Governor Deal was required to sign or veto the bill,

the infosec community in Georgia had about four months to work together to show their opposition.

This is also why it's absolutely essential to have grassroots advocates on the ground, available to educate and activate the public and lawmakers in short order. Thankfully, Electronic Frontiers Georgia sprang into action nearly from the moment the bill was introduced. Local organizations like EF Georgia are incredibly important, and the entire infosec community owes them a debt of gratitude. They informed EFF about the legislation, giving us time to examine and respond. On the ground, they were a credible and local group in the state that lawmakers felt comfortable to work and talk with. They scheduled TV and other press appearances, met with members of the state Senate and House, "worked the rope" (a term for waiting outside the legislative chambers for lawmakers to emerge), held up literal "red cards" during hearings, and hosted a live stream panel.

But the bill still sailed through the legislature, and although it did undergo some positive changes, including exempting terms of service violations, it also acquired its "hack back" amendment in the process.

This only added fuel to the fire, and EF Georgia continued the fight. As a veteran member of EFF's Electronic Frontier Alliance network of grassroots community and campus organizations, they did work that can only be done by those on the ground - but which is absolutely essential.

Out of EF Georgia's efforts came significant public backlash to the bill. Professors organized at Georgia Tech to call upon the governor to veto the bill. Fifty-five tech professionals around the country wrote that, among other things, the bill's exemption for "legitimate business activities" was too ambiguous, leaving researchers who were unconnected with a business (such as academics or independent researchers acting without remuneration) at risk, as well as leaving the definition of "legitimate" too vague.

At the last minute, a hacker group calling itself "SB315" began an ill-advised campaign of defacing local business websites, apparently with the goal of bringing attention to the bill. We called on the group to cease its actions, worried the damage had undone the hard work that advocates, researchers, and more had done to present a reasonable argument, showing instead the "dangerous" side of hacking.

On the last day to sign the bill, in a surprise last-minute veto, Governor Deal wrote: "Consequently, while intending to protect against online breaches and hacks, S.B. 315 may inadvertently hinder the ability of government and private industries to do so." He was absolutely right.

S.B. 315 will likely return next year - and Georgia's infosec community will have to renegotiate the terms of the bill. And unfortunately, there's always a chance that a similar bill will pop up in your area. For now, let's thank the folks of EF Georgia, and remember the lessons of their activism and effort.

If you're interested in helping grassroots efforts like this one, consider joining - or forming - a group in the Electronic Frontier Alliance. Alliance affiliated groups work to educate neighbors, lawmakers, and communities about the importance of digital rights in ways that make the most sense for them, and participation is open to any group that endorses the EFA's simple principles. You can find out more online at eff.org/efa.

A HACKER ADVENTURE IN URBAN EXPLORATION

by Quidnarious Gooch

In the summer of 2015, I decided to go on a little adventuring with a friend. Little did I know I would stumble onto a gem of phone history.



This is the view from the outside. It looked like a normal run down old place, right?

First things first, we decided to hop up on the rooftop. Neat stuff, pretty stylish and *Portal 2*-esque. This was probably a dumb idea in hindsight because we later found the ceiling crumbling in half the building. Whoops.



We got in the place.

As we started mapping everything out, our first assumption was that it was part of a school, because it seemed to be some sort of dormitory. We also found communal showers (not pictured).



Abandoned school



Seeing these seemingly untouched “Do Not Disturb” cards was probably the eeriest part of it all.

We were certainly not the first people there.





Words cannot explain how neglected and totally ignored this place must have been.

We finally found an intact room number placard. It was not a dormitory. We still weren't sure what it was yet, but we now knew that this place belonged to AT&T, although the purpose was still unclear.

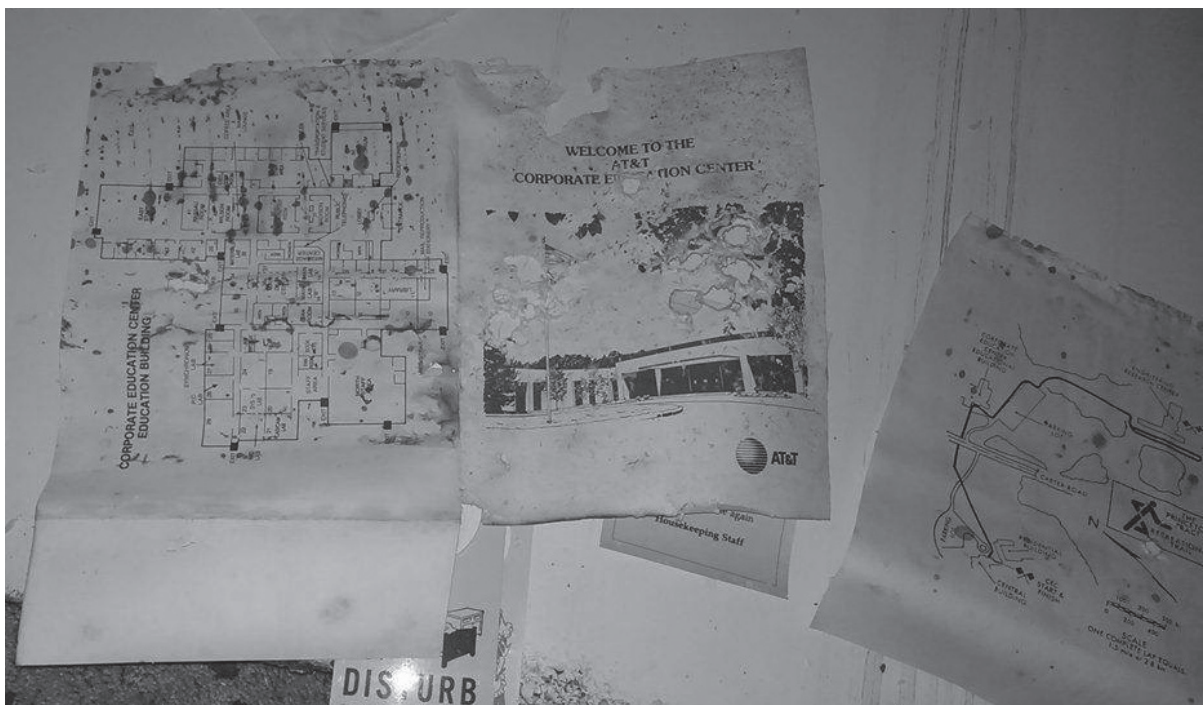
Eureka. A folder left behind with a map to the building. It was a training center for new employees. Whoa.



We later found a map of the campus. The other buildings were already demolished, sadly. We also discovered a dining menu.

We wondered what juicy stuff people had been learning at this place.

Some rooms were completely emptied, while some still had all their furniture like they were simply walked away from for the last time.





These hotel-like rooms with the TVs and lamps and drawers and stuff really gave me vibes like we were near someone... but we weren't.

Books gave us a clue as to when the building had been in use. The Yellow Pages said 1989-1990. We couldn't imagine how this building had been abandoned and fallen apart so quickly. We put the pieces together with more exploration. We concluded that this had been an AT&T phone technician training facility.

This place was eerie. Technology itself is eerie, especially to anyone who was legitimately a phone phreaker and ever themselves dealt with the ominous sounds of the inner switching systems and fiddled with the machinery when they weren't supposed to.



The fact that this place was frozen in time, yet relentlessly showed the effects of time passing, was very cool.

Back in the day was a great time indeed. But now we move forward and readily take on the new dimensions of systems security (or lack of such) in this world.

BEYOND THE SCARE MONGERTAG by StMerry

I am lucky enough to have traveled to Russia for the fifth time in the past few years, and just came back recently after having spent a couple of weeks there. However, it was the first time that I attended ZeroNights in Moscow, and really got to get involved with the local hacker community. I can confidently say that I regret not having done this sooner and it made me incredibly excited and hopeful for the future of our community.

ZeroNights is one of the two larger international conferences present in Russia, along with "Positive Hack Days" which usually happens in spring, and included high-caliber presenters for two days of technical talks and workshops. It also included multiple areas where one could get their hands dirty with car hacking, lock picking, soldering, reverse engineering, arcade gaming, and much more. And, as it should be in my opinion with these sort of gatherings, organizers emphasized the need to stay vendor-neutral and rely mainly on the

community to run the event.

I was already excited about simply attending and learning from others. However, what really stood out for me was that warm feeling of being so welcomed by the community. It only took minutes before I got to know some of the other attendees, and by the end of the two days I had made lifelong friends and saw parts of Moscow from a totally different angle than the one I was ever used to.

In my daily life, I am constantly fed a negative view of Russia, especially on the so-called "cybercrime" scene. And I wanted to take the opportunity to write this article to remind ourselves how the hacker community goes beyond the politics and media accusations. No matter the language barriers, borders, and other obstacles, we keep working with each other, we keep being interested in each other, and we keep being curious together and improving technologies together as well as various social aspects of our lives. To me, the world would be a much darker place were there not a hacker culture, and going to events like this one keeps restoring some of my faith in humanity, a much-needed feeling these days. Stay awesome.

ERRORS

It happens to everyone and, in our Spring issue, it happened to us. The last lines of the article “Breaking Standards” were cut off. (This did not affect the Kindle edition.) Here are the last lines that were printed along with the missing section:

```
To retrieve the password, you proceed with a reverse approach:
$ head -c 10 COLOURB.PI9 | xxd -p | sed 's/\(.\)\(.\)/\2\1/g'
➡ | xxd -r -p
2600@rules
```

Using simple steganography techniques like this one, I recommend that you learn the commands by heart and clear your shell history to leave no visible clue of your manipulation. Of course, you need to properly delete your temporary files too.

I think you get the main idea: breaking the norm and standards, or using exotic or long forgotten ones, can conceal our intention and make the reconnaissance phase far more difficult for potential malevolent people.

The key is to think out of the box. After all, many hacks are based on the assumption that 99 percent of us are using the same predictable tools.

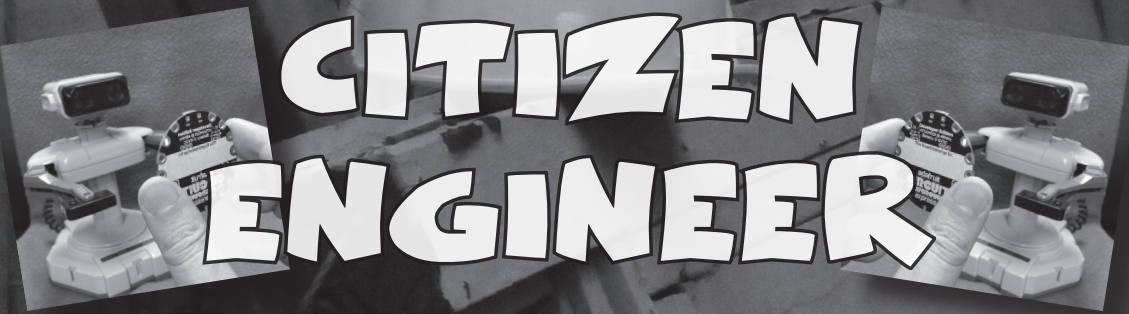
As I’m writing this article, I’m receiving more and more corporate emails assessing the potential impacts of the Meltdown and Spectre security holes on the infrastructures of our customers. To make it simple, every modern computer with a superscalar microprocessor architecture is potentially involved, so hiding sensible data on simpler (emulated) computers might well be a safer choice after all.

All you need is to simply accept that you will get your hands a bit dirty, and learn some strange operating systems or applications you may have never heard of before. But that’s part of the fun, don’t you think?

```
https://www.warhol.org/exhibition/warhol-and-the-amiga/
https://tika.apache.org/
https://github.com/mist-devel/mist-board/wiki
https://aranyan.github.io/
https://www.amigaforever.com/
https://marutan.net/rpcemu/
https://www.dosbox.com/
http://pico-8.wikia.com/wiki/P8PNGFileFormat
http://fileformats.archiveteam.org/wiki/Extended\_DEGAS\_image
http://recoil.sourceforge.net/html5recoil.html
```

We also had an error that *only* affected the Kindle edition. In the letter written by D1vr0c, the line which reads “>var x = 99;” should read “var x = 99;” (eliminating the “>”).

We apologize for any inconvenience or confusion we may have caused.



CITIZEN ENGINEER

"HARD HAT" by marc falardeau is licensed under CC BY 2.0

by Limor "Ladyada" Fried (ladyada@alum.mit.edu) and Phillip Torrone (fill@2600.com)

Hacking a Classic Nintendo R.O.B. Robot

Thirty-three years ago in 1985 (which was considered post-North American video game crash of 1983 due to market saturation), Nintendo released a home-robot. R.O.B. (Robotic Operating Buddy) was an accessory to the Nintendo Entertainment System.

While R.O.B. was appealing, Nintendo only made a couple of games that used his capabilities (<https://en.wikipedia.org/wiki/R.O.B.>).

However, R.O.B.'s success was limited, no more games were released, and R.O.B.s were relegated to closets, his gyro peripherals and claws scattered and lost to the robo-winds.

Revival Efforts

R.O.B.'s movements are commanded by the player using a series of precise flashes from a CRT analog television via a sensor in the robot's head. (It has no direct/wired connection to the NES itself.) But, using an NES on a modern digital LCD TV doesn't work! That's because R.O.B. uses a light sensor in his head which relies on specific flash timing that's a side-effect of how NTSC analog TV works.

Over the years, people have tried to recreate the R.O.B. Controls and there's been some success by Makers who have directly wired to the motor control board in R.O.B.'s base. We took this as a challenge. With the aid of some NES emulation detective work on the AtariAge forums along with Ladyada's NTSC-foo, we have recreated the light control sequence R.O.B. uses to move.

This tutorial will assist you in taking your dusty R.O.B. and making him a useful part of your life.

R.O.B. Buying Guide

If you want to go and buy a R.O.B. here are some hints:

1. You don't need an NES console or game

cartridge. R.O.B. can work alone.

2. You don't need the spinners or other peripherals. The gray "claws" really are not required either.

3. You do want the battery cover for the bottom unless you plan to modify the power in some way.

4. You do want to ask the owner if R.O.B. works with the batteries in and if any gears may be stripped, as this will affect the price you pay.

5. Gear issues can often be fixed, but it may be worth it to buy a R.O.B. that seems in working order.

6. You don't need to buy one of the pristine bundles with or without original packaging unless you are a collector and know what you're spending money on. For this tutorial, only the basic R.O.B unit is needed.

A basic R.O.B. may go for US \$50 to \$100 - don't forget your local thrift shops!

Hacking Optical Control

R.O.B. uses a phototransistor in his left "eye" connected to a Sharp IR3T07 decoder chip. The IR3T07 is undocumented. But some creative folks at AtariAge.com reverse engineered old game cartridges to gather R.O.B.s control codes! Tursi found each command to R.O.B. consisted of 13 bits. The first five bits are an initialization string and are always the same: 00010. The next 8 bits are the command, coded as follows:

- 10111011 - Raises the body up
- 11111011 - Lowers the body down
- 10111010 - Turns the body left
- 11101010 - Turns the body right
- 10111110 - Closes the arms
- 11101110 - Opens the arms
- 11101011 - Turns the head LED on

Each bit is encoded as a green flash on the TV. We started with blinking a bright green LED with 60 Hz pulses ($1/60 = 16.67$ milliseconds) since NTSC has about 60 Hz framerate. No luck. Then we tried to use only the vertical blanking time within the 16.67 microseconds which is 1.5

milliseconds. So out of each 60th of a second, have the on/off bit active for 1.5 milliseconds, then off for the remaining 15.167 milliseconds.

This code was tested with an Adafruit 32u4 Feather and it worked! R.O.B responded to each of the commands!

The LED must be aimed at R.O.B.'s left eye (on the right as you look at him head on) and, unsurprisingly, brighter/narrower LEDs can be farther away than dimmer/diffused LEDs. Once we had some success, we tried other LED colors - turns out it doesn't need to be green. White LEDs and infrared worked just as well. We're not exactly sure why green was used in NES games; perhaps it was the brightest of the three phosphors?

Control Hardware

For our projects, we particularly like infrared because it isn't noticeable to human vision. In the end, we then used an Adafruit Circuit Playground Express (CPX). The CPX is our all-in-one maker board. It has a transmit IR LED with a wide field of view and good transmit power (400mA+). The CPX shows up on your computer as a USB flash drive when connected via a power+data USB cable. Finally, it is programmable via CircuitPython, a language that is easy to use and code that can be changed quickly without installing a tool-chain (like Arduino) and changes do not require recompile. Just copy a new code file onto CPX and it runs.

This makes the parts list very easy - you just need a Circuit Playground Express and a 3xAA battery back or USB cable.

Programming

The code is a relatively short CircuitPython program, and is available in the learn guide. You can copy it from the page or download it from the GitHub link. Save it onto a drive on your local computer as code.py

<https://learn.adafruit.com/control-a-classic-nintendo-r-o-b-robot-using-circuit-playground-express>

To load the code as-is, plug your Circuit Playground Board into your computer via the USB cable. You should see a new flash drive called CIRCUITPY in your list of available drives. In the off-chance your board does not have CircuitPython preloaded, follow the instructions in the guide to load the latest version. Drag a copy of code.py to the CIRCUITPY drive. The program will run immediately.

In the Python code, we set up a function IR_Command, which will do the infrared blinking. There's definitions for the seven 8-bit codes plus the 5-bit init signal. That function performs the blinking as discussed above. If the bit is zero, the function delays 16.5 milliseconds. If the bit is a one, the LED is turned on for 1.5 milliseconds, turned off, and the program waits 15 milliseconds. $15 + 1.5 = 16.5\text{ms}$. The `while True:` loop does the job of polling the Circuit Playground Express inputs and outputs commands appropriately.

If you have issues with R.O.B. not responding to the LED commands, carefully open the head up and remove the paper which restricts light to the left eye and blocks the right eye. This will allow more LED light in and make him easier to control.

It is best to experiment close to your computer with the USB cable still connected to the Circuit Playground Express. Use the serial console REPL to view debug information: printed info that the program has started and then (x, y, z) readings from the Circuit Playground Express accelerometer.

Hold your Circuit Playground Express about 12 to 18 inches from R.O.B.'s head with the IR LED not blocked by your finger and aimed at R.O.B.'s left eye (on your right). Don't shake the Circuit Playground Express yet - hold it steady.

Now press the A button with a finger. R.O.B.'s arms should open wide (if closed). Press button B on the front of the Express and his arms should close. Hey, my robot works!

The other controls are a bit trickier - some practice will help. If you turn the Circuit Playground Express board clockwise, R.O.B. should twist one way. Turn it counterclockwise and he should move the opposite way. It may take some practice as the board is reading the changes in acceleration relative to the pull of the earth. Short, quick movements work best while keeping the IR LED aimed at R.O.B.'s head. Tricky but doable.

The final movement involves a quick up movement to have R.O.B. move his torso up. The silver USB connector should be moved up in a short quick movement (without twisting). R.O.B. should move the whole body/arm assembly up. A quick downward movement towards the ground should move the torso down. Again, keep the IR LED pointed at R.O.B.'s left eye. It may take some practice.

Once you have the basics down, you can unplug the USB cable and use the battery pack to make a portable solution. Go have fun with your robot!

Video: <https://www.youtube.com/watch?v=ffAuebA5WAo>

Good night and good luck.

Re-Purposing Old Technology and Ideas for Fun and Emotional Profit

or

Get Off My Lawn, You Technological Whipper Snappers!

by John Q. Sample

My friends and I come from a blue-collar background. While I was growing up, our families didn't usually have a lot of money for frivolous things that we didn't need. The money earned was money for food, bills, etc. Occasionally, a luxury could be afforded, but that was few and far between. When those luxuries could be afforded, they tended to be perhaps not the best version of what was available. For example, when things like a television or a computer were purchased, it wasn't the most modern version of what may have been around at the time.

While growing up, our families made due with what they had. We grew up in a time where technology started moving from a coveted luxury to a necessary commodity. From that necessity and near poverty grew a coupon cutting ethic that allowed us to maintain a certain cyberpunk status quo, and at the same time prevented us from unintentionally becoming economically mandated Luddites. When Linux became an option, it was amazing for us. We had the ability to use older hand-me-down, throwaway versions of computers, and be able to functionally use up-to-date versions of software to peruse and be a part of what was happening at metaphorical breakneck speed socially and technologically on the Internet. We were able to be a part of the wonderful thing that was happening to the world with technology.

If you flash forward to today, you find technology has stabilized to a reasonable price. One can purchase a Raspberry Pi computer for \$25, or a laptop for \$150. It's not unreasonable for someone without the luxury of large amounts of money to be involved in the technological experience anymore.

One thing that lack of finances and the need to be a part of what was happening provided was a hardwired internal need to use throwaway technology. It's ingrained in us to never throw out anything. We have to find a new way to use that piece of equipment. We must recycle it. In this writer's opinion, it's an ethos that's missing from the current technologically

adept society. We've included everyone in the process, but at the expense of privacy and at the behest of corporate interests.

We have become a marketing product and it's acceptable to give our money over and over again to corporations who do not have our best interests in mind. If one wanted to convey a message, one would have to do it in such a fashion that would provide an opportunity for those same corporations to make even more money through ads posted around our independent media messages. If we just looked proverbially behind us, we would see a glut of technology long forgotten that provides us a means to employ a message and at the same time do it in a fashion that provides us privacy. In essence.

Why reinvent the wheel? We can accomplish this all by re-purposing old technologies in new ways.

Take, for example, cassette tape technology. Now I know retro technologies in regard to audio recording seems to have its aficionados, but we're talking about re-purposing this technology here. And if it becomes the go-to for hipster audiophiles, the better for us who want to use the technology in different ways because the prevalence of the technology provides us more of an opportunity to find what we need to work with it. Tapes were at one point the go-to for data storage before the abundance of the long gone floppy disks became available.



Figure 1: Commodore 1530 (C2N) Datasette.

Not to mention that the technology was prevalent, as it was the go-to for everyone who listened to music. Cassette players were prevalent everywhere. In homes and vehicles, cassette players were the standard way to listen to music.



Figure 2: An example of a “boombox” cassette tape player.

With the advent of CD technology, and ultimately MP3s, taking over as the standards for consumption of music, tape players went the wayside. Relegated to attics and corners of dusty basements. But they’re still there. Collecting dust, perhaps. But they still exist in people’s possession. Which means that you can get them free or very cheaply. Why not resurrect them from their demise for use today? With a combination of free programs such as Coagula and Audacity, one can use them to encode text messages into audio files for later viewing. In a world where the NSA sniffs all of our Internet traffic encompassing it all into “metadata,” I pose the idea to use older technology to circumvent that invasion of privacy. One can simply open up a copy of Microsoft Paint and type their message into the top of an image with a black background and white lettering.

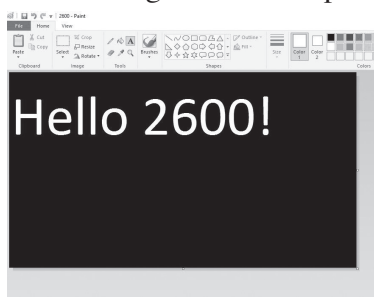


Figure 3: Using Microsoft Paint to type a message with a black background and white lettering.

Save the .bmp image. That image then can be processed through Coagula and an audio file created in the form of a .wav.

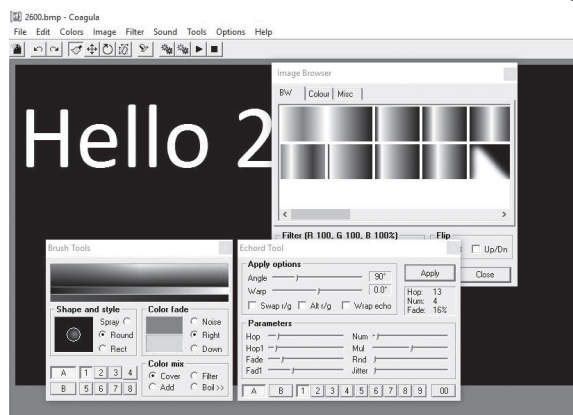


Figure 4: Using Coagula to render a .wav file.

That audio file can then be transferred to an audio cassette. When played back and recorded into any audio editor capable of viewing a spectrogram of your .wav file, such as Audacity in this case, the intended recipient of the message would then view the spectrogram and after adjusting the spectrogram settings for clarity, will then be able to see the message.

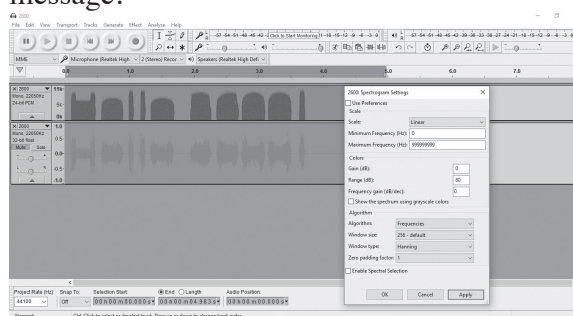


Figure 5: Viewing the spectrogram and the message.

After recording the message, if one were fortunate enough to come across another piece of technology relegated to the trash heap - a four-track recorder - one would be able to ultimately record that text message subliminally “below” another audio file, increasing the chances of the original text message remaining a secret between the recorder and the intended recipient.

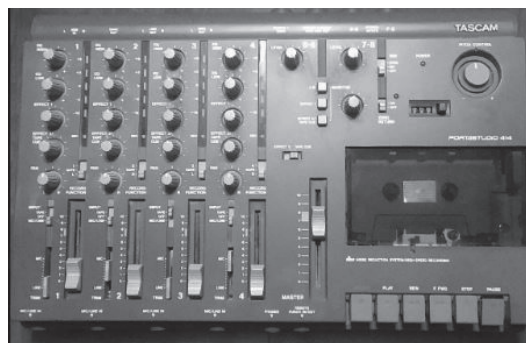


Figure 6: An example of a four-track recorder.

This isn't necessarily a "how-to." The ideas and technology presented in this article aren't new. (That is with the exception of the author's suggestion of implementation.) That's the point. My suggestion is one that should imply the use of older technologies and "outdated" ideas for unintended use, not necessarily direction on what one should use or how to use it. The aforementioned was just a suggestion. And while some would consider hacking older technologies thought to be obsolete to be "bush league," I point to SCADA systems and their counterparts, suggesting that when one discounts those types of technologies as options, one leaves open the opportunity for

nefarious actors to use those technologies in whatever ways they see fit. To discount the idea is to leave one open to unintended consequences. To remember the older technologies and use them is analogous to understanding the older technology, its security implications, and, at the same time, allowing for a "rebirth" of the technology for use.

There's a whole world of forgotten instructions and technologies written off as obsolete that can ultimately still be used for purposes not yet imagined by those innovative minds in our hacker community. Good luck finding the right platform and happy hacking!

Hacking: Quick and Easy

by haplesscheese

You're the aspiring hacker - interested in Internet hacking communities, clubs, and events, but with little hacking background or knowledge. You want to get your hands on your computer and do something you can be proud of - and have the community be proud of you. How? Penetration testing is an experienced occupation, requiring years to hone skills and find out what works best. Besides, computers and operating systems are constantly advancing, and old systems are rapidly becoming obsolete. You need something now.

0x01 Choosing a Job

As far as we're concerned, there are five types of hacks: DoS (i.e., SYN flooding, distributed DDoS), web exploits (i.e., SQL injections, URL manipulation, XSS, CSRF), wireless hacks (i.e., Wi-Fi vulnerability scanning, Wi-Fi key cracking), social engineering (i.e., phishing, keylogging), and malware. For something you can do at home right now, let's choose to create a web exploit. Our goal is for a successful SQL injection (where, in place of a variable, text that represents SQL commands will be executed) to be played out on our target.

0x02 Gathering the Tools

To do our job, all we'll need is a web browser. However, one of the best penetration testing operating systems on the web is Kali Linux. Kali contains many tools that would be useful to the aspiring hacker. My personal setup includes VirtualBox running a copy of Kali. You can find links to download VirtualBox and Kali in the References section at the end of this article.

0x03 Selecting a Target

To find a vulnerable target, we'll use Google dorks (search terms that bring specific results for a domain). Lists of popular Google dorks can be found online, but we'll just use "inurl: \"login.aspx?id= \" intitle: \"admin\"\" (without the quotations on the ends) to get all websites that contain \"login.aspx\" in the URL and \"admin\" in the title. Most of these will be vulnerable due to them sending queries to the database directly in the URL.

A typical URL query might look like this:

```
SELECT * FROM Users WHERE
➤ Username = '' + UserInput
➤ AND Password = '' + PassInput;
where "UserInput" is the username
provided by the user and "PassInput" is the
password provided by the user.
```

An injected query could then look like this:

```
SELECT * FROM Users WHERE
➤ Username = '' + ' OR ''1=1'
```

➡ AND Password = '' + ' OR
➡ ''1=1';

This statement would effectively login the user to the first row in the table "Users". This makes it extremely easy for us to break in.

0x04 SQL Injection

Once a vulnerable target has been found, we'll begin our process. In the Username and Password boxes, type ' OR ''1=1'. We

might now be greeted with a confirmation of login, along with our username. We are in.

(Note: SQL injection might be blocked on the server that you use.)

0x05 References

VirtualBox: <https://www.virtualbox.org/wiki/Downloads>

Kali Linux: <https://www.kali.org/downloads/>

Thoughts On Cryptocurrency

by Frizzank

What does cryptocurrency have to do with hacking? Well, it turns out, quite a bit. I am quite proficient with computers, and my experience ranges from my first Apple SE computer (well, my parents') to my latest builds which heat my house in the winter and overheat it in the summer. That's right. I have free heating - and that is what got me into crypto in the first place.

This article is not about how to get rich, mine cryptocurrency, or even promote a viewpoint. (I do have a website, which I suppose I can shamelessly plug in here: cryptominingtalk.com. Feel free to go there and learn about how to heat your home like I do.) No, this article is about what I have learned and how I regained a long lost love of life through the process of discovery and exploration (OK, I'm exaggerating, but only a little bit).

First off, mining can be done with a GPU. Although I was already good with computers, I had never built my own, by myself. Taking the plunge a few years back, I ordered parts online, and built one - one with six graphics cards connected to one motherboard. I learned to control and understand how voltage and clocks work on a GPU, as well as how to modify and flash a BIOS. I learned how to modify memory timings. I had all kinds of problems at first, and I went to sleep scratching my head a few times. But I got through it, by trying and trying over and over. I never gave

up. I learned about myself. And I did it all over again. I also learned about electricity and proper wiring. How to be safe and up to code. I learned about networking.

I just wanted to share that once I found that new hobby, I was hooked. And I was happy. It doesn't really matter what it is - shortwave radio, robotics or programming, whatever - as long as you find something that truly interests you and that stimulates your hacker spirit. One that we are all born with.

Life today is quite often prepackaged and user-friendly, and opportunities to find new things that interest us as we grow older become hard to come by. We have to search for them. Boredom and routine is our enemy. Go to conferences or meetings and interact with people.

Through my website, I get to interact and help people from all over the world, including places like Venezuela, where people want and need to learn about bitcoin and the general crypto technology. They use that info to free themselves from oppressive government monetary policies and to survive. Sure puts thing into perspective. When you need U.S. dollars to import goods, but it is illegal for you to buy them, crypto can sure come in handy. I just use it to heat my house and garage. But it also heats my heart.

It's not about having a meaning in life. It's simply finding meaning in the things you do. My hacker spirit stayed dormant for too long - and finally it has awakened again. I hope yours does too. Stay Cheeki Breeki, my friends.

Dev Manny, Information Technology Private Investigator “Hacking the Naked Princess”

by Andy Kaiser

Chapter 0x15

The magic of money had just given me a new friend named Terry.

Terry made a good living being homeless in the broken industrial park of West Rapids. He had shelter if it got cold, since while many of the buildings were closed and shuttered, they were rotten enough that there were ways to get in. He had plenty to eat. Since he had mapped out locations of dumpsters and trash cans from surviving businesses, his menu was more defined by his mood than availability. While I was savoring my daily cup of noodles, this guy ate sushi multiple times per week.

Terry also liked to talk.

“I got what I need,” he said, extending skinny arms to take in the whole of the crumbling buildings around us. “Got time to enjoy and I tell you why. I plan it out, son. Plans get you success. You don’t plan, then that’s a plan for failure. Like you, now, where you’re gonna get success if I help you get inside your RedAction place, because you’re planning to give me two hundred fifty bucks.”

“Two fifty? Was that the number?”

“US dollars,” he nodded confidently. “That’s your plan.”

One trip to an ATM later, I was counting bills into his palm, which was lots of cups of noodles. I stopped at one fifty.

“Hey now,” he said.

“I seem to remember the original deal was less. You’ll get the last hundred after we do this.”

“Son,” he said, shaking his head sadly. “You don’t understand your position -”

“I do, Terry. You just made a hundred and fifty for bragging how you eat better than I do. You’ll get another hundred for some actual help.”

He tilted his head and squinted at me, then grinned and gave a sharp nod.

“This thing,” I said, waving the USB stick from P@nic. “I have to plug this into a

computer inside the RedAction building. It can be any computer, but I need to get inside the place to do it. Then I’ll leave. Unnoticed.”

“Not a problem.”

“Well, it’s not that easy. This is a secure place. They probably have cameras -”

“Yeah, they got ten. On each side, more on the roof. And doubled up around the front entrance and back loading dock.”

I was surprised. “How do you know that?”

He stared at me with a look that said I was wasting his time which from a courtesy standpoint shouldn’t need to be said because even though he was homeless he wasn’t going to wait for me to get with the program and the only reason he was still standing there was because I was holding his money.

“You sound like you’ve done this before.”

“Yeah, nah. But I know people who care about those things.”

After coming up with a plan that was admittedly more Terry’s idea than mine, a few minutes later saw me confidently walking towards the RedAction building with the eyes of multiple security cameras tracking me.

Except for the security cameras that Terry had proudly pointed out to me, the outside of the large brick building was unremarkable. Inside was a different story. A heavy door opened into a clean, spacious hallway. A receptionist sat on the other side of a wall, looking at me through a small sliding security window. On my side of the wall, another heavy door stood closed. A red light glowed on a card reader mounted next to the door. This was the problem - I needed to get through that door. P@nic’s USB stick was burning a hole in my pocket - I wanted to get in, find a PC, drop off P@nic’s present, and get out of there.

I looked around. I didn’t see any company logos, mottos, or anything that said RedAction. But this was definitely the place. They even kept their headquarters anonymous.

Breaking her attention away from a paperback book, the receptionist slid open the security window and said, “Welcome to Product

Management Group. Who are you here to see?"

Here we go.

P@nic said she'd hit RedAction hard with a DDoS attack from her botnet, and it would hit right now. That should be enough to saturate the company bandwidth and bring Internet access offline.

"I'm here about the web problems," I said. Keep it high-level, keep it simple. She'd fill in the rest.

"Oh, that's so good!" Relief in her voice, she rolled her eyes upwards. "I'm glad they called someone in to help. They told us it was another Microsoft update that went crazy. I guess they need help."

While I'm happy to blame Microsoft for everything, from buggy forced OS updates to rainy weather, I tried to understand what the RedAction admins were thinking. They had to know they were under a DDoS attack. They couldn't quickly stop it, and this type of attack didn't conceal itself. Maybe it was better to tell the users something they could understand and not worry about. They'd gain breathing room to work through the issue without users and bosses who would freak when they heard the word "attack." In short, lie and downplay the severity. An oldie but goodie.

"You can go to IT," the receptionist said, and I felt confident until she picked up her phone receiver. "Let me get security for you."

I needed to get in there alone. There was no way I could do what I needed with their security watching me the whole time I was here.

"No, don't bother them," I said quickly, and her finger froze over the phone touchscreen as she looked up at me politely. "I can just head back there myself. I know where to go."

"Oh, I know," she gave me an apologetic smile. "But it's policy. All visitors must be escorted. I'll get security to take you to them."

I watched helplessly as she hit an extension and spoke quietly into her phone, then turned to me cheerfully. "On their way now!"

"Thanks."

RedAction's security door buzzed and the red LED turned green. The door swung open to reveal a mountain of a security goon. His muscles were armed with a gun, baton, mace and other tactical gear hanging from a Batman-worthy utility belt. He stood with a military poise. He examined me up and down and nodded, his eyes flat. He looked like he didn't like to smile.

"Good afternoon, sir. You're with IT?"

"Yeah, I just need to get to -"

The main entrance door behind me flew open. It hit the wall with a slam as Terry burst in and fell onto the floor in his rush. He climbed back to his feet and reached both arms to the heavens.

"His arrival brings a dark world!"

The security goon refocused his dead stare on my newest cash-motivated friend.

"Whoa there, sir." Goon stepped past me and went to tower over Terry. He held both hands up apologetically, trying to crowd Terry back towards the door. "I'm going to have to ask you to leave, sir. I can escort you out of this building -"

"Your life is suffering, wretched, infernal! The Great Old Ones breathe life eternal!"

Terry's face was red, his arms were flailing, and I even saw spittle fly from his lips as he yelled. Full credit to the man, Terry was good at improv insanity.

The guard was focused on managing this clearly crazy intruder, responding politely while also corralling him back. I looked behind me. The receptionist was watching the scuffle with wide eyes, and had slid closed her small access window.

The security door behind me was still open. I used it.

Terry's distraction should buy me a couple minutes, enough time to introduce P@nic's USB stick to an unoccupied computer. Terry was ranting louder and was now trying to push back against the guard. My hope was that RedAction didn't want any attention, so they wouldn't want the police called, like if a guard assaulted someone trying to enter the building. Even with video evidence in their favor, RedAction had secrets inside of secrets, and any outside investigation would be prevented with all possible effort. I hoped.

I stood in a hallway that ran straight ahead with periodic doors accessing large cubical farms. From the multitude gray squares, several curious heads were sticking up above the cube walls like groundhogs in human form. Listening to the ranting lunatic near the front entrance, they didn't even notice me. I ducked into the first cubical room and began to scan right and left, looking for unoccupied desks with computers.

I skipped the first couple I found. One was right near the hallway and too easily seen by

anyone going past. Another had a PC sitting on the desk, and what I needed to do had to be more covert. A third had a steaming mug of coffee next to the keyboard, so I guessed the owner was close and probably returning soon.

Then in the next cube over, I saw a floor-standing tower PC shoved under the desk. It was powered on, the monitor patiently displaying a logon screen. The chair was shoved against the desk and no coat or personal items were visible.

Terry's voice began to fade away. It sounded like the guard was finally getting him outside. I had seconds to get this done and get out, before the office went back to normal and I could more easily be caught.

I dropped to the floor and wiggled to the PC, fishing out P@nic's USB stick from my pocket at the same time. Against the wall in the corner of the cube, I craned my neck around in the gloom to look for open USB ports in the back of the PC. I cursed quietly when I saw all ports were being used. Seriously, what did a generic RedAction user need? Mouse, keyboard, and what else? Four locally-attached printers? I picked a cable at random and yanked it out. I gritted my teeth at the cheery "BONG-bong" from the PC as it noticed I unplugged something, and wanted the world to know. It did it again as I inserted P@nic's USB stick into the slot I'd just freed up.

I'd done it. Whatever tool P@nic had me install would hopefully activate, and she could do her magic and properly infiltrate this place and bring them down. Like right now. All I needed to do was to get out of here before I was noticed.

"Um, *excuse me*."

From under the desk, I stared back at a pair of sensible shoes that had just entered the cube along with legs, all of which I assumed

belonged to the cube's owner.

I slid out and glanced up at the woman as I did so. She was staring down at me, fists on her hips.

"What are you doing?" she spoke through a sudden hammering of my heart.

"Just working on the Web issue," I said, trying to keep the problem generic and high-level, pitching my voice like the bored tech I hoped she was used to dealing with. "An ethernet thing. Your DNS cable was loose."

"Oh, okay. Can I work or not?"

"Yeah, sure. All set. Thanks." I hopped up, smiled briefly, and started back the way I'd come.

I walked down the hallway towards the entrance that was now my exit. Other employees were navigating the hallway, most carrying fresh refills of coffee, and we all did the head-bob of acknowledgment as I made my way past them. At the last one, we made eye contact and my stomach dropped.

I'd just nodded to Oober's "mom." The lady who'd lied about herself and Oober, who first pulled me into this case, and I'd just made direct eye contact with her. If she recognized me, big problem. I knew she worked for RedAction. I didn't think I'd actually see her again.

A couple days' beard growth and a lack of hair combing wasn't much of a disguise. Still walking, I casually glanced around and behind me to see if my face had triggered anything from her.

She had stopped in the middle of the hallway and looked frozen in place. She turned slowly to look back at me, her eyes wide.

"Dev Manny!" she screamed. "That's the investigator! Security! Anyone!"

There was a chance she remembered me. I turned and ran.

They're here! Our latest hoodie release combines our popular pullover hooded sweatshirt with our most popular design: the infamous blue box schematic.

Only \$29.99 plus shipping at store.2600.com



2600 logo on the front, blue box schematic on the back

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under \$200 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, *email us* at happenings@2600.com or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA**. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

July 20-22 The Circle of HOPE Hotel Pennsylvania New York City, New York hope.net	September 22-23 World Maker Faire New York New York Hall of Science Queens, New York www.makerfaire.com
August 4-5 Maker Faire Tokyo Big Sight Tokyo, Japan makezine.jp/event/mft2018	October 5-7 DerbyCon 8.0 Marriott Louisville Louisville, Kentucky www.derbycon.com
August 9-12 DEF CON 26 Caesar's Palace Las Vegas, Nevada www.defcon.org	October 12-14 Maker Faire Rome Fiera di Roma Rome, Italy www.makerfairerome.eu
August 9-13 Trans Hackmeeting Le Goutailloux Tarnac, France trans.hackmeeting.org	October 19-21 PhreakNIC 22 Clarion Inn Murfreesboro, Tennessee phreaknic.info
September 6-7 GrrCON DeVos Place Grand Rapids, Michigan www.grrcon.org	November 30 - December 2 Hack3rCon 9 Holiday Inn Hotel & Suites Charleston West South Charleston, West Virginia www.securewv.com

*Please send us your feedback on any events you attend
and let us know if they should/should not be listed here.*

Marketplace

Events

THE CIRCLE OF HOPE. A Hacker's Dozen. The 12th incarnation of the Hackers On Planet Earth series, taking place at the Hotel Pennsylvania in New York City July 20-22, 2018. We have expanded space this year! By the time you read this, it'll either be over or about to happen, so check hope.net for the latest updates!

For Sale

SECUREMAC.COM is offering popular anti-malware app MacScan 3 to help protect Mac users from malware, spyware, and ransomware. Download a 30-day trial directly from SecureMac.com and enter code 2600 at checkout for special savings.

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at HackerWarehouse.com.

DEFEND YOUR WI-FI. Coaxifi delivers Wi-Fi over your home's coaxial cabling to eliminate dead zones. Reuse your existing router to send Wi-Fi farther. Check out our new WiFork kits! 10% off with promo code "SUP2600". coaxifi.com

PORTABLE PENETRATOR. Find WPA WPA2 WPS Wifi Keys Software. Customize reports use for consulting. <https://shop.secpoint.com/2600>

\$2 WILL BUY A FORMER ONE-WAY FUNCTION! <https://www.amazon.com/Prime-Number-Factors-that-Solve-ebook/dp/B079XYZ596> Prime Number Factors that Solve $N = p * q$ - Kindle edition by Bobby Joe Snyder. Download it once and read it on your Kindle device, PC, phones, or tablets. Use features like bookmarks, note taking, and highlighting while reading Prime Number Factors that Solve $N = p * q$.

HACKERSTICKERS.COM now carries cDc merchandise, accepts bitcoin, sells lock pick sets, bawls energy mints, and an awesome lineup of hacker clothing including the new Johnny Cupcakes x HackerStickers collaboration Hacker Big Kid Shirt. Get all the goods at HackerStickers.com.

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Available in two quantities: \$36.99 per 12 pack or \$53.99 per 18 pack of half liter bottles plus shipping. Write to contact@club-mate.us or order directly from store.2600.com.

Help Wanted

JOIN THE [HTTPS://CODEFOR.CASH](https://CODEFOR.CASH) community and earn money with freelance programming jobs. All hats welcome!

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the 2600 site in mp3 format! Your feedback on the program is always welcome at oth@2600.com.

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1020 products listed which include 219+ VPN's, 192 messaging and 117 file encryption apps. These are just a few of the 27 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome.

AUSTIN HACKERSPACE: A shared workshop with electronics lab, laser cutters, 3D printers, CNC machines, car bay, woodworking, and more! \$60/mo for 24/7 access to all this and a great community as well. Open House and open meetups weekly. 9701 Dessau Rd, Austin, TX <http://atxhs.org/>

Services

ASPIRING TO BE THE MOST ETHICAL TECH SHOP IN THE WORLD, Technoethical.com offers the largest catalog of hardware products certified by the Free Software Foundation (FSF) to Respect Your Freedom (RYF) [fsf.org/resources/hw/endorsement/technoethical]. As a user of Technoethical devices, you have the maximum control over your computing, being able to use, copy, modify, and distribute all the bits in the operating system and, when possible, even at lower levels, such as the boot firmware. The shop sells laptops and servers pre-installed with a fully free (as in freedom) BIOS replacement and GNU/Linux-libre distributions verified and endorsed by the FSF. All x86_64 devices serviced and sold have Intel's intentional backdoor, the Management Engine [u.fsf.org/2g0], completely removed. As the only shop that sells phones with Replicant [replicant.us] pre-installed, you can be the first hacker on your block to own an Android-based device with an operating system that can be compiled completely from source with no proprietary blobs. You can also buy from Technoethical a diverse array of WiFi adapters that work with drivers and firmware that are fully hackable and operate also in the Access Point mode. Moreover, Technoethical provides installation/liberation services for all computers that are also sold as products. You can ship your compatible computer to Technoethical, or ask the team to organize a workshop in your local hackerspace or free software event. With 4 years of experience on the market, Technoethical is operated by a geographically distributed team of hackers from North America, the European Union, Russia, and Australia that closely follow the software freedom principles of the GNU project. Use the coupon code 2600MAG to receive a 5% discount on all Technoethical products. Order today and join Richard Stallman among the many happy customers of Technoethical!

SQUIDIX provides serious discounts for fantastic web hosting for 2600 readers. We love our clients and they love us. Our 2600 promotion will give you a Super Squid hosting platform for only \$26.00 for the first year, then only \$9.95 per month when paid annually. Sign up today and get free domain or domain renewal. This offer valid for any new accounts in 2018 and includes a free CPanel transfer of one existing site. Sign up at www.squidix.com

GET YOUR HAM RADIO LICENSE! KB6NU's "No Nonsense" study guides make it easy to get your Technician Class amateur radio license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. The PDF version of the Technician Class study guide is free, but there is a small charge for the other versions. All of the e-book versions are available from www.kb6nu.com/study-guides/. Paperback versions are available from Amazon. E-mail cwgeek@kb6nu.com for more information.

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMES? Stand up for your rights! Be calm, cool, and collected: "I respectfully invoke all of my Constitutional rights, officer. I do not consent to any search or seizure, I choose to remain silent, and I want to speak to a lawyer." Remember basic game theory and the Prisoner's Dilemma: nobody talks, everybody walks. Consult with a lawyer experienced in defending human beings facing computer-related charges in California and

federal courts. Omar Figueroa is an aggressive Constitutional and freedom defense lawyer with experience representing persons accused of unauthorized access, misappropriation of trade secrets, and other cybercrimes. He is a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and is willing to contribute pro bono representation for whistleblowers and peaceful hacktivists. Past clients include Kevin Mitnick (million-dollar-bail case in California Superior Court dismissed), Robert Lyttle of The Deceptive Duo (patriotic hacktivist who exposed elementary vulnerabilities in the United States information infrastructure) and Vincent Kershaw, reported member of Anonymous indicted for his alleged participation in a DDOS action against Paypal. Also, given that the worlds of the hacker and the cannabis connoisseur have often intersected historically, please note I also specialize in cannabis legal compliance and can help you navigate a complex maze of marijuana-related laws and regulations. Please contact Omar Figueroa, at (415) 489-0420 or (707) 829-0215, at omar@stanfordalumni.org, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472.

PANIC STATION is a quarterly zine put out directly from prison that focuses on original writing, hacking, music, punk rock life, and prison shenanigans. 2600 readers can request a free issue by writing a letter to me. Submissions welcome, please only send letters (no stamps, etc.)! Vincent Veneziani, #249067G/1079583, 215 S. Burlington Rd. - SWSP, Bridgeton, NJ 08302.

HAVE YOU SEEN THE 2600 STORE? Plenty of features, hacker stuff, and all sorts of possibilities. We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. We have an increasing amount of digital download capability for the magazine and for HOPE videos. Best of all, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's digital forensic examiners hold the prestigious CISSP, CCE, CEH, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data nationwide from many sources, including computers, external media, tablets, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Our principals are co-authors of *Locked Down: Practical Information Security for Lawyers*, 2nd edition (American Bar Association 2016), *Encryption Made Simple for Lawyers* (American Bar Association 2015), and hundreds of articles on digital forensics and an award-winning blog on electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

SKEPTICAL OF GITHUB? sr.ht is an in-progress software suite for hosting open source projects that's more in tune with the hacker way. sr.ht is more modular and more flexible, with features like mailing list driven development and full virt build automation with KVM. Interested in helping test the beta? Reach out to SirCmpwn: sir@cmpwn.com

INTELLIGENT HACKERS UNIX SHELL: Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from \$5/month, with a money back guarantee. Lifetime 26% discount for 2600 readers. Coupon Code: Save2600. <http://www.reverse.net/>

ANTIQUÉ COMPUTERS. From Altos to Zorba and

everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. <http://www.vintagecomputer.net>

LOCKPICKING101.COM - a locksport community driven by lock picking hobbyists and locksmiths alike. New to lock picking or want to advance your skills or help others learn? Just head over to LockPicking101.com and say Mr. Picks sent you!

DOUBLEHOP.ME is an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and transparently exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to. We accept Bitcoin and offer automated order processing! Use promo code COSBYSWEATER2600 for 50% off (<https://www.doublehop.me>).

Personals

PENPALS WANTED: Fellow hackers! I'm incarcerated and need someone to keep me in touch and fresh on the hacking scene. The library here is horrific at best with absolutely no resources for my interests. With less than a year before my release, I am looking for someone to bounce ideas off of, ask questions, and talk about common interests with. I am from Dallas, TX and will be there when released. I have been looking into Bitcoin & mining. I also have fascinations with the dark web, methods, and carding. I LOVE GLITCHES!!! Please reach out to a fellow hacker before my release. I am determined to surround myself with like minds. Please don't send books! I can't get them unless they come directly from the publisher or bookstore (amazon.com and online stores are okay). Any & all financial direction and/or suggestions are greatly appreciated. If you know of ways for me to start an income once I'm released, please, please, PLEASE let me know! Just write me if any of this catches your attention or if you want to know more about me. R. Murphy #2148621, 6999 Retrieve Rd., Angleton, TX 77515.

SEEKING PENPALS. I'm incarcerated and looking for penpals. I've been down for over two years now and the boredom is really starting to set in. My hometown is Cleveland OH and that is where I will be released in a few years. Before the Feds kidnapped me, I worked network operations for an ISP. Being out of tech for so long now, I'm starting to feel antiquated. It would be nice to have penpals willing to discuss tech, and send technical docs. No Internet access here and hardly any resources for keeping up with tech. I have many other interests too, including general aviation, health/fitness, snowboarding, travel/foreign cultures, etc. I'd be happy to share the many crazy stories of what really happens in prison. Respond to the address below. Do not use address labels or stickers; it will be rejected/returned. Thank you! Daniel Nieberding 61030-060, Federal Correctional Institution, PO Box 1000, Loretto, PA 15940.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.

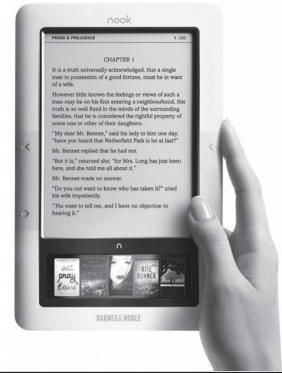
Deadline for Autumn issue: 8/21/18.

Want to Become a Digital Subscriber to 2600?

Head to digital.2600.com for the latest



In addition to the good old-fashioned paper version, you can now subscribe in more parts of the world than ever via Google Play, the Nook, and the Kindle. We're also constantly increasing our digital library of back issues and Hacker Digests.



2019 HACKER CALENDARS

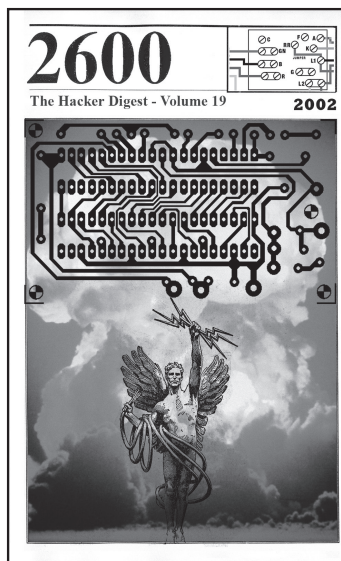
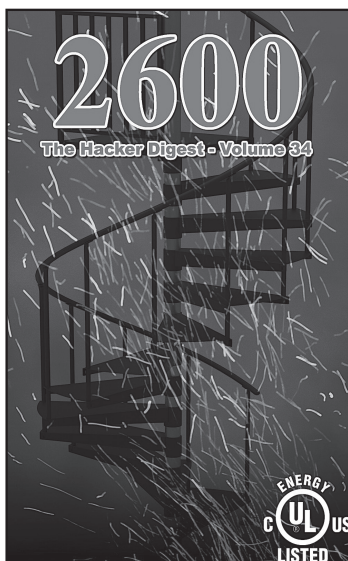
The 2019 Hacker Calendar is about to be released! (At the time of this printing, we were still putting it together so the picture here is of 2018.)

Each month features a 12"x12" glossy photo of a public telephone from somewhere on the planet, and nearly every day marks something significant in the hacker world.



Get yours when they're released in late July! Visit store.2600.com

The Lifetime *Hacker Digest* Subscription



We now have 29 years of 2600 digitized with more being added every three months! By becoming a lifetime subscriber, you'll get all of our existing *Hacker Digests*, plus a newly archived one every quarter, along with a brand new digest once a year for as long as you or we are around. \$260 gets it all. (Existing lifetime subscribers to the analog edition can get all of this for only \$100.)

*Left: Volume 34 from 2017
and Volume 19 from 2002*

Visit store.2600.com and click on Downloads/PDF.

Editor-In-Chief
Emmanuel Goldstein

S

Infrastructure
flyko

Associate Editor
Bob Hardy

T

Network Operations
phiber

Layout and Design
Skram

A

Broadcast Coordinator
Juintz

Cover
Dabu Ch'wald

F

IRC Admins
beave, koz, r0d3nt

Office Manager
Tampruf

F

Inspirational Music: Bessie Smith, Childish Gambino, Gang of Four, Graham Nash, Louis the Child, P. Miles Bryson, Monkey Mafia, Jumpin Jack Frost, Valve Sound System, Pusha T, DJ Eva, Lemon D

Shout Outs: Mamoudou Gassama, James Shaw Jr., Jason Seaman

2600 is written by members of the global hacker community.

**You can be a part of this by sending your submissions to
articles@2600.com or the postal address below.**

.....
2600 (ISSN 0749-3851, USPS # 003-176) is
published quarterly by 2600 Enterprises Inc.,
2 Flowerfield, St. James, NY 11780.
Periodical postage rates paid at
St. James, NY and additional mailing offices.

POSTMASTER:

Send address changes to: 2600
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:

2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:

U.S. & Canada - \$29 individual,
\$50 corporate (U.S. Funds)
Overseas - \$41 individual, \$65 corporate

BACK ISSUES:

1984-1999 are \$25 per year when available.
Individual issues for 1988-1999
are \$6.25 each when available.
2000-2017 are \$29 per year or \$7.25 each.
Shipping added to overseas orders.

**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

Copyright © 2018; 2600 Enterprises Inc.

ARGENTINA
Buenos Aires: Bellagamba Bodegon, Armenia 1242, first table to the left of the front door.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499, Capital Federal. 7 pm

AUSTRALIA
Central Coast: Central Coast Leagues Club (ground floor, outdoor area). 6 pm
Melbourne: Captain Melville, 34 Franklin St. 6 pm
Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

BELGIUM
Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL
Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA
Alberta
Calgary: Food court of Eau Claire Market. 6 pm
Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia
Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.
Vancouver: International Village Mall food court.

Manitoba
Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick
Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland
St. John's: Memorial University Center food court (in front of the Dairy Queen).

Ontario
Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA
Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

COSTA RICA
Heredia: Food court, Paseo de las Flores Mall.

CZECHIA
Prague: Legenda pub. 6 pm

DENMARK
Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

FINLAND
Helsinki: Forum shopping center (Mannerheimintie 20), food court on floor zero.

FRANCE
Paris: Burger King, first floor, Place de la Republique. 6 pm

GREECE
Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND
Dublin: At the entrance to the Dublin Tourism Information Centre on Suffolk St. 7 pm

ISRAEL
***Beit Shemesh:** In the big Fashion Mall (across from train station), second floor, food court. Phone: 1-800-800-515. 7 pm
***Safed:** Courtyard of Ashkenazi Ari.

ITALY
Milan: Piazza Loreto in front of McDonalds.

JAPAN
Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

KAZAKHSTAN
Astana: CheckPoint Brasserie, Koshkarbayeva St 34. 8 pm

MEXICO
Chetumal: Food court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and

the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS
Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY
Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsø: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm
Trondheim: Den Gode Nabo. 7 pm

PERU
Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm
Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES
Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

POLAND
Krakow: VR Cafe, Dolnych Mlynów 10. 8 pm

RUSSIA
Moscow: RNDM, Podkopayevskiy Pereulok, 7. 7 pm
Murmansk: Rock and Roll Music Bar, pr. Lenina, 11. 7 pm
Petrozavodsk: "Good Place" anti-cafe, pr. Pervomayskiy, 2. 7 pm
Saint Petersburg: Krasnodonskaya Ulitsa, 4. 7 pm

SWEDEN
Stockholm: Champlucks at Stockholm Central Station.

SWITZERLAND
Lausanne: In front of the MacDo beside the train station. 7 pm

THAILAND
Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM
England
Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero Shopping Center (near Piccadilly Circus), front entrance on Coventry St. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Coach and Horses on Thorpe Rd. 6 pm

Scotland
Edinburgh: Beehive Inn on Grassmarket. 6 pm
Glasgow: Starbucks, 9 Exchange Pl. 6 pm

Wales
Cardiff: Rummer Tavern opposite Cardiff Castle.
Ewloe: St. David's Hotel.

UNITED STATES
Alabama
Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Arizona
Phoenix: Lux Central, 4400 N Central Ave. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm
Tucson: BlackRock Brewers, 1664 S Research Loop #200. 6 pm

Arkansas
Fort Smith: Fort Smith Coffee Company, 1101 Rogers Ave. 6 pm

California
Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (behind Pizza Hut). 7 pm
Chico: Starbucks, 246 Broadway St. 6 pm
Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar. 6 pm
Monterey: East Village Coffee Lounge. 5:30 pm
Petaluma: Starbucks, 125 Petaluma Blvd N. 6 pm
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center near street level fountains. 6 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado
Fort Collins: Dazbog Coffee, 2733 Council Tree Ave. 7 pm

Connecticut
Wallingford: Panera Bread, 1094 N Colony Rd. 6 pm

Delaware
Newark: Barnes and Nobles cafe area, Christiana Mall.

Florida
Fort Lauderdale: Grind Coffee Project, 599 SW 2nd Ave. 7 pm
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Jacksonville: Kickbacks Gastropub, 910 King St. 6:30 pm
Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Tampa: Cafe at Barnes & Noble, 213 N Dale Mabry Hwy
Titusville: Playalinda Brewing Co., 305 S Washington Ave.

Georgia
Atlanta: Lenox Mall food court. 7 pm

Hawaii
Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho
Boise: BSU Student Union Building, upstairs from the main entrance.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois
Champaign-Urbana: Lincoln Square Mall food court.
Chicago: O'Hare Oasis on 294 behind the bank kiosk. 8 pm
Peoria: Starbucks, 1200 West Main St.

Indiana
Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Indianapolis: City Market, 2nd floor, just outside Tomlinson Tap Room.
West Lafayette: Jake's Roadhouse, 135 S Chauncey Ave.

Iowa
Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 627 W 2nd St.

Kansas
Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Biting Ave.

Louisiana
New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine
Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland
Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts
Boston (Cambridge): Starbucks, The Garage, 36 JFK St. 7 pm
Waltham: The Telephone Museum, 289 Moody St.

Michigan
Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota
Bloomington: Mall of America food court in front of Burger King. 6 pm

Missouri
St. Louis: Arch Reactor Hacker Space, 2215 Scott Ave. 6 pm

Montana
Helena: Hall beside OX at Lundy Center.

Nebraska
Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada
Elko: Uber Games and Technology, 1071 Idaho St. 6 pm
Las Vegas (Henderson): SYN Shop, 1075 American Pacific Dr Suite C. 6 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire
Keene: Local Burger, 82 Main St. 7 pm

New Jersey
Somerville: Dragonfly Cafe, 14 E Main St.

New York
Albany: Starbucks, 1244 Western Ave. 6 pm
New York: The Atrium at 875, 53rd St & 3rd Ave, lower level.
Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina
Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).
Raleigh: Morning Times, 10 E Hargett St. 7 pm

North Dakota
Fargo: West Acres Mall food court.

Ohio
Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.
Columbus: Front of the food court fountain in Easton Mall. 7 pm
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.
Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

Oklahoma
Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon
Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania
Allentown: Panera Bread, 3100 W Tilghman St. 6 pm
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, food court outside Taco Bell. 5:30 pm
Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.
State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico
San Juan: Plaza Las Americas on first floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm

South Carolina
Myrtle Beach: SubProto, 3926 Wesley St, Suite 403.

South Dakota
Sioux Falls: Empire Mall, by Burger King.

Tennessee
Knoxville: West Town Mall food court. 6 pm
Nashville: Nashville Software School, 500 Interstate Blvd S #300. 6 pm

Texas
Austin: Whole Foods 2nd floor pavilion, 525 N Lamar Blvd. 7 pm
Dallas (Addison): Dunn Brothers Coffee, 3725 Belt Line Rd.
Houston: Ninfa's Express seating area, Galleria IV. 6 pm
Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont
Burlington: The Burlington Town Center Mall food court under the stairs.

Virginia
Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm
Lexington: Collaboratory, 18 East Nelson St, #103. 6 pm
Reston: Refraction, 11911 Freedom Dr. 8th Fl. 7 pm
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington
Seattle: Cafe Allegro, upstairs, 4214 University Way NE (alley entrance). 6 pm
Spokane: Starbucks, 4727 N Division St.
Tacoma: Tacoma Mall food court. 6 pm
Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.

Wisconsin
Madison: Fair Trade Coffee House, 418 State St.

URUGUAY
Montevideo: MAM Mercado Agrícola de Montevideo, Jose L. Terra 2220, Choperia Mastra. 7 pm

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, 2600 meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle!

More American Payphones



Peru. Who needs a booth when you can just fasten a phone directly into the wall? Found in an alley in Plaza de Armas in Lima where we're told the wild street dogs pick fights with pampered police dogs in Bane masks.

Photo by Count Famicom



Costa Rica. Operated by Condicel, this card-only model was found in the city of Liberia by a grocery store. And now you all know the phone number....

Photo by Steve/Funky49



Cuba. Now this is the kind of respect a payphone deserves. While it seems like something from another planet, just looking at this phone booth makes you feel safe. It's like being in a cave. Found in Remedios and operated by Etecsa.

Photo by Sean from Canada

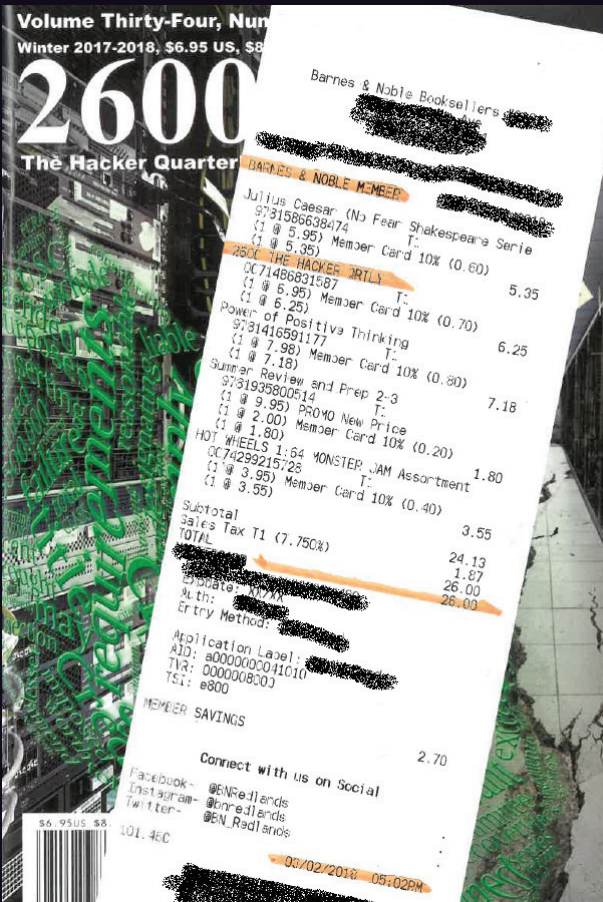


Bahamas. Found in the downtown part of Nassau, this scene looks like it could be in Queens, New York. In fact, someone even scrawled "Queens, NY" on the side of one of the phones! Operated by BaTelCo, not to be confused with Batelco (look it up).

Photo by Doug Lippert

Visit <http://www.2600.com/phones/> to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos



It takes a special kind of skill and often dozens of trips to the store to get your total to add up to this magical number. But to do this *while* buying our magazine is something truly worthy of note. Congrats to **Alejandro** for unlocking this achievement.

As a sequel to last issue's picture in this space, we thought this image of New York City's "2600" bus from a different angle would be pretty cool. Thanks go to **Benjamin** who shot this from deep inside the former Trump SoHo. We honestly didn't even know buses had numbers on their roofs!



If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a 2600 t-shirt of your choice.