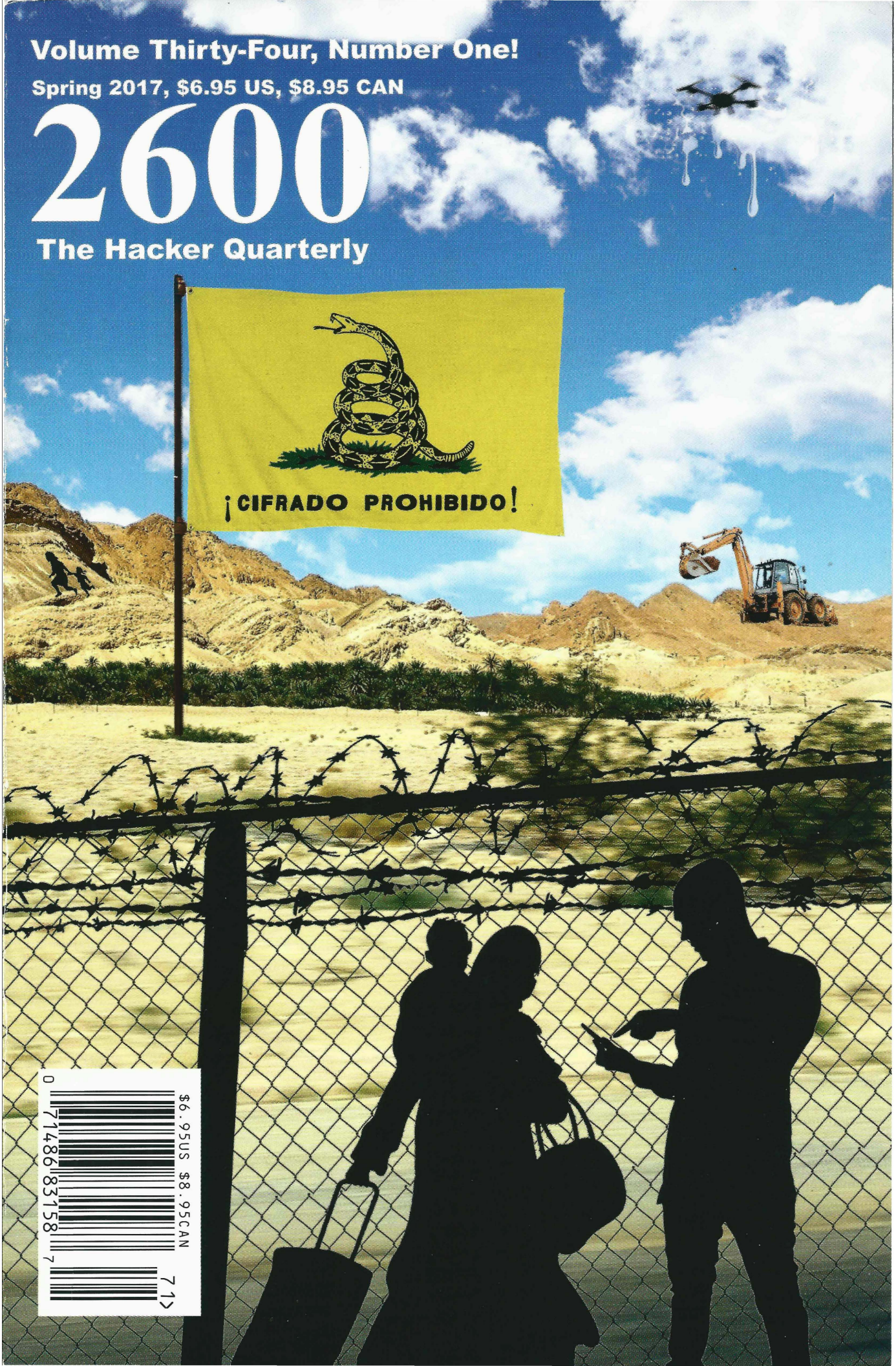
Volume Thirty-Four, Number One!
Spring 2017, $6.95 US, $8.95 CAN

2600

The Hacker Quarterly



0 71486 83158 7
$6.95US $8.95CAN
71

Latin American Payphones

Peru. Yes, in this country you can apparently just stick a payphone onto a tree if that works for you. This one was seen in Ollantaytambo in the Sacred Valley of the Incas. ***Photo by Victoria Dietz***

Peru. A bit more of a traditional approach found in Iquitos. Telefónica is a Spanish company that operates throughout South America.

Photo by Andova Begarin

Colombia. Located in Chia, we're impressed with the combination cord and chain that keeps the receiver from wandering.

Photo by Dallas Luce

Mexico. This phone was found in the mountains over Puerto Vallarta. It only works for local calls and the cost on the receiver says $3 unlimited, meaning three pesos (around 15 American cents).

Photo by Dwayne Jenkins

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 (Do not send us links as photos must be previously unpublished.)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)

Chemicals

#resist

A Price for Truth

What a bizarre and crazy ride this year has been in such a short period.

To say the Trump administration is unlike anything we've experienced before would be a massive understatement. We speak for many when we say that we were expecting a degree of crackdowns, closures, regressions, anger, fear, and the like, but what we've gotten so far leaves us almost speechless.

Almost.

We've been through a good amount of administrations. It's hard to believe, but Ronald Reagan was the president when we first started publishing. Since then we've gone through two Bushes, one Clinton, and an Obama. At no point can we say that we've lived under a hacker-friendly administration. But that was never really something we expected. Ignorance is pretty much the theme when it comes to government understanding of technology and all of its nuances, doubly so when you inject social issues and rebelliousness into the mix. Reading through our pages over the past 33 years, you see that we've always been fighting an uphill battle, whether it be testifying before Congress, condemning raids on hackers and overreaching by federal authorities, or campaigning against the latest ill-advised piece of legislation.

Let us be clear for those who may feel we have a specific political agenda. Far and away the worst threats came under the Clinton administration, when the government finally seemed to get a grasp of what technology was all about - and then sought to control it in every way imaginable. We had the Clipper Chip, the Digital Telephony Act, the Communications Decency Act, and a long list of others, all of which were fought - and many of which were overturned after lengthy court battles. And under the Obama administration, we saw more clampdowns on leaks using the Espionage Act than with all other administrations *combined,* as well as the laying of groundwork for massive surveillance that helps make widespread abuse in the future a foregone conclusion. While the level of understanding and sophistication of technical discussion may, in fact, have risen during these administrations, this didn't always translate into a better scenario for the people.

The point is that no matter who is in charge, we're going to be fighting these battles. And sometimes the people you see as having a better grip on things will wind up causing us more problems precisely because they believe they have it all figured out. In short, this is not about Democrats and Republicans. At least, not on this level. We know that no matter who happens to be in power at the moment, we're going to have our work cut out for us in trying to stop bad things from happening and in educating people as to what the best policy is regarding technology and privacy - and why.

However, all of this default antagonism that we're always prepared for in any administration doesn't begin to cover what seems to be ahead on the Trump agenda. In an incredibly brief time, we've seen the press defined as the enemy of the people, the demonization of undocumented immigrants with a nationalistic zeal that should worry anyone who's ever picked up a history book, statements that unfairly castigate entire religions and nations, racial insensitivity, embracing of conspiracy theories, lack of meaningful dialogue, favoritism of an epic proportion resulting in unelected individuals being catapulted into positions of great power, huge and damaging conflicts of interest that are willfully ignored, unprecedented incompetence in vital posts, lack of knowledge or interest in history and world affairs, threats of military action within our own borders, a wanton disregard for the fragile environment of our planet, extreme insecurity and hostility when confronted with criticism, accusations with no supporting evidence... we could keep going, but odds are you're already aware of most of this. And all of these are ingredients vital to the rise of fascism, something we've never really experienced in our country. Sure, we have problems that need to be dealt with, as does any country. *How* such issues are handled is what defines a society and we are far from alone in being exceedingly troubled with what has happened so far.

Perhaps the core of what's most disturbing here is an attitude that somehow Trump and his ilk believe they don't have to abide by the same rules as everyone else. *"[A]s you know, I have a no-conflict situation because I'm president... it's a nice thing to have... I have something that others don't have..."* We've seen this assumption of privilege rear its ugly head before in Trump's previous life. It's up to all of us to make sure we remind him and his supporters at every opportunity that this is not how it works. Because once it is, any hope for a functioning free society is lost.

We all know it's possible "legally" to come up with all kinds of words to allow great injus-

tices to be gotten away with. But morally... that's another story. That is where we must apply our efforts without any hesitation.

This brings us to the infamous tax returns, the ones that Donald Trump believes nobody cares about, the ones that he can continue to hide from the American public. It's no secret that the majority of people *do* care and, while legally he can hide them from us while lying about the reasons, morally it's indefensible. How can anyone assert that we don't have the right to know what is being claimed on this form while we're entrusting him with such great power and responsibility? Mistruths and cheating will quickly be revealed if they are there. So too will the *absence* of these things, a revelation that will help the healing process begin and instill some much needed trust.

While members of the public can claim the right of privacy in not sharing such information, it's pretty much an unwritten rule in our society that our leader should display his honesty in this public manner. Yes, it's unwritten, meaning he doesn't *have* to do it. But the consequences of rejecting this tradition, as with many other voluntary actions that are expected of a president, could have a very detrimental effect on our society... and the resulting ripples would be felt throughout the world. Being in such a privileged position means *sacrificing* some of one's privacy - as has been done for decades - in the interests of open and transparent democracy.

Clearly, he has not been willing to do this. And, equally troubling, his allies are prepared to prevent this information from becoming public. In February, Republicans voted unanimously to block Democratic efforts to obtain Trump's tax returns. Yes, they have the power to obtain them and put this all to rest, but they chose to continue covering it up instead.

Last year, we half jokingly offered $10,000 to anyone who could get us these elusive returns for then candidate Trump. Now that he's the "leader of the free world" with more scandals and cover-ups in the first few weeks of his administration than most presidents have had in their entire terms, this can no longer be thought of as remotely funny. We all have the right to know just who is running things. That is why we are reinstating our offer and making it potentially much bigger.

Here's the deal. We're offering ten grand to anyone who gets us the returns in question before any other media outlet. If you want to add to this amount (and we know that many people do), simply email **trump@2600.com** and tell us how much you want to add. That's it. If we receive the documents we're asking for, we will contact you and ask you to make good on your pledge in the method of your choice. Once the full amount has been received and awarded, the tax return(s) will be released.

If you want your email to be more secure, we suggest using PGP. Our PGP key can be found in the submissions section of our web page. (Yes, metadata will still show that you emailed us, but nobody else will know what the contents of your email are. We've already gotten a ton of email to that address containing everything from pledges to condemnation of who we are and what we stand for.)

We will continue to add pledges to the total amount. If someone actually sends us one of the tax returns (which, in all honesty, we believe is extremely unlikely), we will have it authenticated and keep it safe while we collect the pledges and then work out an anonymous way to issue the payment. We will do everything we can to keep the names of leakers and pledgers confidential. This is a responsibility we don't take lightly.

A couple of important points: we do *not* want people breaking the law to obtain these documents, trying to hack the IRS, or anything like that. There are numerous individuals who already have legitimate access to this information. That is the key. Also, this applies to any unreleased tax returns within the past five years, *not counting 2016,* as those presumably haven't been filed yet and we don't know what will happen on April 15th. Also, we're only doing this for as long as Trump is in power, since that's as long as this remains urgently relevant.

Now, of course, we know this is going to really bother some very powerful people and that we could easily be prosecuted for even attempting to do this. But there comes a point where a choice has to be made and, for us, the choice was a simple one. We could just do nothing and watch from the sidelines. Or we could call upon people with access and a conscience to do the right thing and shine some light on the truth. The hacker community is quite familiar with this kind of decision; we've seen some real heroes step forth in recent years to get us the truth while enduring great sacrifices as a consequence. We've also seen it throughout our entire existence on more localized levels as kids are disciplined by schools and employees punished by companies simply for revealing the unwanted truth about one thing or another.

While it's admittedly terrifying to prepare to take on this kind of an adversary, our words over the years would mean very little if we didn't step forward if we had even the slightest chance of getting closer to the truth.

New U.K. Surveillance Laws - Time to Get Serious About Security

by Dr. G

You may have already heard - but in case you haven't - the United Kingdom is expanding their surveillance powers through the Investigatory Powers Bill that was passed in Parliament and given royal assent in November 2016. It is now the law of the land, at least in the U.K., and allows for some interesting powers. Every website visited by every U.K. citizen will be stored for a full year by every ISP operating within the country, and that data will be offered up on a silver platter to the government whenever they make a request - all without the need for a warrant. Presumably, this will apply to any person using the Internet within the U.K. since there isn't a real method of determining who is a citizen. This same storage also applies to mobile apps as well, so you can be certain the phone companies will be involved in the shenanigans. This is supposed to be limited to the metadata and Internet connection records, but we all know how quickly governments step over the line when these types of actions are involved. This same bill allows the government to legally hack into computers, monitor phone conversations, and use the other normal surveillance techniques most law enforcement agencies already use. This last piece requires a warrant from a panel of judges and the Secretary of State so, at least on the surface, they are making it look tough to acquire. The European Union's courts have stepped in to block this overreach of government surveillance, but the Brexit will likely keep the new laws in place. OK, no real new news there except that governments are continuing to expand their spying on people inside and outside of their borders.

So for all the newbs, those who have forgotten how to protect themselves, and anyone else, here are some ways to keep yourself safe next time you travel through the U.K., or anywhere else for that matter. I'm intentionally keeping this from being a technical, step by step article. You're smart enough to figure out the details. I'll just give you some crumbs to lead you in the right direction.

First up: Internet activity. Tor is a pretty obvious choice here. You could use one of many free or paid for VPN services: just search for "VPN services" if you want a listing. This is great for watching Netflix from a restricted location, but you never know if the providers of these VPN services have been compromised or strong-armed by the government. So, even though it may appear secure, it might just be an illusion. One hop for all your data isn't a great choice, which is why we have Tor. Now, I'm not a big fan of Tor because a lot of human traffickers and child exploiters use it to hide their activities. But, in this case, Tor is likely your best option to keep anyone from spying on your perfectly legal and legitimate Internet activity. You can download and install the Tor browser, then use it anytime you think your privacy is at risk. There are also a few Tor-based apps for Android and iPhone that give you the same capabilities. Check their website for the latest options. Unless you're a criminal, Tor is probably overkill for your everyday Internet activity and can slow you down considerably. If you just want to encrypt your web traffic without any concern for the monitoring of your browsing habits, you can use the HTTPS Everywhere add-on for Firefox, Chrome, and Opera which, essentially, makes much more of your traffic encrypted and unreadable. And if you are concerned about a search engine tracking your

search habits, navigate over to a service like Disconnect Search. Just be warned: one of their developers used to work for NSA.

Phone conversations and text messaging are even more common than Internet activity, so we'll cover that next. There's always the Blackphone from Silent Circle, but that's a steep price to pay since many of the capabilities are available as free apps on Android and iPhones. Signal Private Messenger from Open Whisper Systems can handle both of these tasks, assuming the person you are communicating with is also using the Signal app. Similar to Lavabit, Signal uses end to end encryption and Open Whisper Systems doesn't have access to any of your messages, message content, voice conversations, call data, metadata, or anything else. Everything is private between you and the other party. Edward Snowden promotes this app and - love or hate him - that is a pretty big endorsement. Honestly, I like to make encrypted phone calls to my wife just to make NSA think there is some big secret that they don't know about.

So what about email? This is probably the most difficult. Email encryption is a clunky operation, even for technically savvy people. There are some third party solutions you could use; one of the Snowden NSA leaked documents stated that they haven't been able to break encrypted emails by users of Zoho or similar online email services. But I'm not a big fan of these solutions because it puts someone else in the middle that I may not be able to trust at some point down the road. Enter PGP. Yes, it's been around since the early nineties, but it is still a solid method of encryption that is used worldwide. You can start using it right away with the GNU Privacy Guard (aka GPG), but it will take a bit of time to get it set up and, depending on your email client, will probably require some copying and pasting of the encrypted contents before sending the message on its way. As with other forms of communication, the receiver will need to be able to decrypt the contents if they want to read your message, so you may be limited in this scope unless everyone you talk to is as security conscious as you.

If you want to take it to another level, encrypt your entire phone. The latest versions of the iPhone and Android operating systems provide full disk encryption capabilities for the phone's internal memory and additional SD card storage, when available. Both Apple and Google have gone on the record - in a somewhat veiled fashion - to say that there are no back doors to their operating systems that can bypass this encryption capability. OK, if that is true, then any person or government who wants to analyze your phone won't have much to do, that is, as long as whatever password you are using isn't something they can easily break. Different countries have different laws about whether you would need to hand over your password, so do some research before you travel. The U.S. Supreme Court ruled in 2014 that police can't search phones without a warrant, but you may be forced to give up the password once the warrant is issued. I suppose you could pretend you forgot the password.

And you should also encrypt your computer as well. If you don't already have TrueCrypt installed, you are missing out on a capability that the same Snowden leaked file indicated the NSA couldn't break. TrueCrypt mysteriously shut down a few years ago and it was widely suspected that they got hit in the same way as Lavabit, but their software is still available and, apparently, still unbreakable. I always keep a few encrypted containers on my systems to keep private information private. You should do the same.

You get the basic idea. People want to monitor your communications for a lot of different reasons and, while I have no problem with governments spying on each other, I don't want any of those governments spying on me. If you want to see what I am doing, get a warrant. And even then, good luck breaking through the encryption of my stuff because I'm pretty sure I'll forget my password. These tips should help you secure most of your common communication, since NSA seems to be stuck when it comes to using the solutions in this article. That should make all of us do the happy dance, even the really bad dancers, which, let's face it, is most of us. Happy encrypting!

References

- http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
- https://techcrunch.com/2013/10/07/disconnect-search-built-by-ex-google-and-ex-nsa-engineers-lets-you-use-google-bing-and-yahoo-without-tracking/
- http://www.cnn.com/2014/06/25/justice/supreme-court-cell-phones/

VOICES IN THE SKY—
SATELLITE COMMUNICATION METHODS


https://niskanencenter.org/wp-content/uploads/2016/11/spacetrafficahead.jpg

by Monican

There are more than one thousand active satellites orbiting the Earth, several thousand more that are abandoned, and around 20 deep space satellites and spacecraft. There are plans in the next three years to launch nearly a thousand more, many of which belong to new smallsat fleet operators like OneWeb, Planet Labs, and BlackSky Global. In this article, I will cover the current methods that satellite operators use to communicate with satellites and spacecraft, security issues, and the future of laser communications and what it means for us Earthlings.

One thing that every single satellite has in common is a need to communicate with the Earth, and this is done with radio-frequency (RF) communications in several frequency bands. As many readers probably know, the Federal Communications Commission (FCC) in the United States and equivalent regulators in other parts of the world have to carefully police usage of the electromagnetic spectrum so that people don't interfere with each other and with critical services like ambulance radios, air traffic control, and radio stations. This creates a problem for satellite operators who have to deal with multiple regulatory agencies since satellites broadcast across continent-sized swaths of the Earth. This wide field of transmission also creates security issues around eavesdropping which I'll cover more below. The other problem that arises from RF comms is how slow they are. For example, when NASA tries to download data from the Mars Science Lab rover, speeds can be as low as several kilobits per second. One of the causes of this low data rate is the wide beam angle over such a great distance which wastes energy, and the low-frequency nature of UHF, X-band, and S-band radios.

UHF, the lowest frequency transmission spectrum of those three examples stands for "Ultra High Frequency," so why do I say they are low-frequency? When compared to the frequency of visible light, their limitations become apparent. Visible light is three orders of magnitude higher frequency than traditional radios, operating in the terahertz band. This allows not only faster communication because more information can be encoded in a given unit of time, but also much tighter beam-width, which cuts down on wasted energy sending photons elsewhere other than your target.

Thus there are two huge benefits to using lasers to communicate over long distances rather than RF: higher data throughput and lower energy needed to transmit. One more benefit is very important to the militaries of the world: the tighter beam-width means eavesdropping on the signal is much more difficult. Here's an example: the LADEE spacecraft which went to the Moon and spent a year orbiting it tested out lasercomms between the Moon and Nevada. The laser beam hitting the Earth was only six miles in diameter, centered approximately on the trailer-sized receiving telescope. This means that anyone trying to listen in on this conversation would have to be within six miles of the receiver in the desert, which would be very easy to spot and prevent. Lasercomms are also immune to jamming unless the adversary is directly in view of the telescope, which is much harder due to the vastly narrower field of view compared with traditional RF.

The main barrier to implementing Earth-space lasercomms is interference from the Earth's atmosphere. Water vapor and other gases in our air diffract visible light (and infrared and UV) and only recently have scientists developed reliable single-photon detection, ensuring that even if the light scatters upon entering the atmosphere, reception is still possible. Receiving telescopes on spacecraft are restricted to very small sizes, which means that an Earth-based transmission must blast quite a bit of power at the spacecraft. The way operators get around the low power limits of the space-to-Earth transmissions and the small size

of the receiver on the spacecraft is by having a very large cryogenically cooled receiver on the Earth with a really powerful transmitter. In some sense, energy for a terrestrial transmitter is "unlimited" compared to the tight power budgets of a spacecraft. So the powerful ground stations allow the other end to be quite small and low power.

Another drawback of optical laser communications is weather dependence. Clouds block visible and infrared light, so the ground stations have to be in very dry, clear areas, such as the high deserts of Chile or the arid regions of New Mexico, Spain, and Australia. Due to this limitation and the still experimental nature of lasercomms, future satellites and spacecraft will still need to have an "old fashioned" X-band, S-band, or UHF antenna, but these will increasingly be seen as just emergency backups rather than primary systems.

The higher level of security that comes from the tighter beam-width of lasers still has classic weak points: the terrestrial communications network used to send these signals between the desert transceiver and end users will still rely on classic encryption and suffer from any problems experienced by the network on Earth.

These developments will have a noticeable impact on our lives in the coming decades. Vastly higher data rates between the Earth and space, or between satellites in orbit, will improve our global communication network as well as allowing far more scientific data to be downloaded from future scientific missions. The militaries of the world are busy developing lasercomms to make eavesdropping more difficult and get around jamming. Lasercomms will also be used more for point-to-point communications on the Earth in locations where it is not feasible to wire fiber optic cable.

260026012602260326042605260626072608260926102611261226132614261526162617261826192620262126222623262426252626272628262 **Lockbox PIN Code Generator** 926302631263226332634263526362637263826392640264126422643264426452646264726482649265026512652265326542655265626572658265926

by Victor

Months ago, an associate was commenting on the oddities of a physical key lockbox. I'm sure you're familiar with the type of lockbox typically used by realtors which are intended to securely store a house key; opened with a PIN code or dial combination lock. So my associate's "uncle" had "forgotten" the combination or acquired one of these things and was trying to brute force the box.

The lock box in question was of the push-button variety, opening with a numeric PIN. While the PIN length can vary, he knew that the PIN on his lockbox was four digits long. Trying up to 10,000 PINs sounds like quite a boring task, right? But wait, there's more. The lockbox in question was made by Supra and, after some querying, he learned there were deficiencies in the design of this lockbox that significantly reduced the number of unique PINs. The PIN couldn't repeat any numbers and the order in which the pin was entered didn't matter (e.g. 1234 was the same as 4321)!

My associate started searching, but couldn't find a ready-made list of PINs. His initial attempts at generating a list weren't quite right and I was drawn into the idea of solving this with some Python.

I'll give you the executive summary and you can jump straight to the code. We're generating the PINs as a string, so it can be padded with leading zeroes to the necessary length. Converting the PIN to a list allows us to sort. Sorting the PIN's characters is what addresses the fact that the order in which a PIN is entered does not matter. There's also a check to eliminate PINs which use any digit more than once.

The check to eliminate PINs using any digit more than once might look strange to those less familiar with Python syntax.

```
if [c for c in pin if
        ➥ pin.count(c) > 1]:
```

This is really a one-liner for creating a list. See "List Comprehension" in the Python docs. It iterates the characters in the PIN and returns a list containing only characters that exist more than once in the PIN. Python's IF evaluates to True only when the returned list contains something.

It was reported to me that the resulting list of PINs and a six-pack later, his uncle was triumphant! I suspect the Supra lockbox model in question was mechanical in nature (as opposed

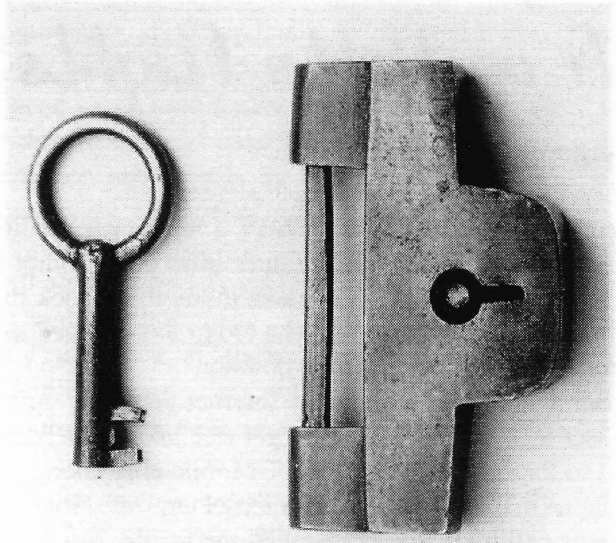
to having some electronic guts), which led to these strange properties. The number of viable PINs was shockingly low, as you can see below. What I hadn't thought of is that because PIN order doesn't matter, a five-digit PIN is the most secure - more or less digits reduces security. Remember that when brute forcing, you're likely to hit on the winner halfway through the key space, so halve those numbers below to get a better idea of just how few tries it's likely to take.

It might be worth taking a minute to tinker and search for vulnerabilities with any lockbox you plan to use. I suspect those industrious fellows in the Lockpick Village are having a chuckle at this.... I'm certain there are more egregious physical flaws in these types of products.

This is a fine start for PIN-generating needs which I've reused a couple of times already. Happy hacking and I'd like to give a nod to $@LV@Ti0N for bringing this puzzle to my attention.

PIN Length	Number of Unique PIN Combinations
1	10
2	45
3	120
4	210
5	252
6	210
7	120

```
#!/usr/bin/env python
#
# Create a pin list to crack a supra key box.
#
# Supra key boxes (I am told) have the unique feature of not requiring
# the owner to remember the order in which a pin is entered (!).
# Additionally numbers in the pin can only be used once (e.g. 2234 is
# invalid because 2 appears twice).
#

if __name__ == '__main__':

    pin_length = 5      # <-- Adjust pin-length here

    i = -1
    end_pin = int('9'*pin_length)
    pin_list = []

    while i < end_pin:
        i += 1

        # generate pin with leading 0's; convert it to a list; sort it
        pin = str(i).zfill(pin_length)
        pin = list(pin)
        pin.sort()

        # skip pins with reoccurring chars; pins already in our list
        if [c for c in pin if pin.count(c) > 1]:
            continue
        if pin in pin_list:
            continue

        # add our pin to the master list of valid pins
        pin_list.append(pin)

    # print results
    for pin in pin_list:
        print(''.join(pin))

    print('There are {pincount} combinations.'.format(
            pincount=len(pin_list)))
```



"Lock and key" by Japan via The Metropolitan Museum of Art is licensed under CC0 1.0

A LOCK WITH THE KEY NEXT TO IT

by Ckjbgames

Hello, *2600* and its readership. I am here to address the insecurities of my school network. These insecurities are absolutely ridiculous and I cannot believe how honestly horrible this network's security is. Even for a middle school. My school's security is like taking a lock, securing it in the right way, but then leaving the key right next to it so that anyone can access all of your important documents.

First off, all of the computers run Windows 7, except for (of course) iOS devices and Chromebooks. This is ridiculous. Even though Windows 7 might have a better UI than 8 and 10, there is *no mainstream support* as of almost a year ago. That might not seem so bad, but it gets worse.... I have several old *2600* issues that I read through (volumes 20-22), and several of the Windows XP-era security hacks still work on these computers!

For example, the network admins know nothing about the Google Translate proxy hack, I presume. I can access any blocked website via this method, and no one has done anything about it. Some kids even have no restrictions on accessing the Internet! I am one of the unlucky people who got an account with Internet restrictions. This laziness is inexcusable: you cannot just add Internet restrictions to some of the accounts and leave the rest with full access to the Internet!

Another thing to think about is that we can insert USB flash drives without being denied permission. This is insanity. Also, even better, you can use Windows Explorer and go into directories including C:\, Program Files, and even a directory full of assembly language code. I am not even kidding. It is that bad. I bet that the admins thought that we wouldn't think about it.

Another thing that you would normally think was a good security measure is laid to waste. So, you are denied access to the Command Prompt. An easy security measure that would make most give up at this point. However, they probably did the stupidest thing possible: forgot to deny access to Windows PowerShell.

You should probably know what PowerShell is: it's a utility that can do what Command Prompt can do and more: you can write shell scripts. I haven't found PowerShell ISE yet, but I have found PowerShell. All you do is search for "Windows PowerShell" in drive C:\ and a single folder named "x86-windows-powershell-" and then a bunch of possibly encoded characters that look like gibberish. I didn't care to analyze any; I just wanted to get to PowerShell. In the folder is a shortcut to - guess - Windows PowerShell. From here, you can access the network, not as an admin, sadly, but you can still run "net" commands. You can also change settings and possibly (I haven't tested this) access VBS. So much for a lock when the key is right next to it....

I have not reported any of this to any figures of authority, and none of my friends know about these loopholes, except for the Google Translate one. I would like anyone reading this to think about what the point of a lock would be with the key right by it, or with the combination just a few feet away.

Hacking Free Wi-Fi on Delta Flights

by David Libertas

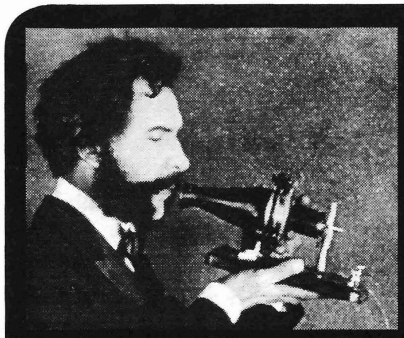
I was on a Delta Airlines flight and connected my netbook to the Wi-Fi. I remember reading in *2600* that some airlines open up full Internet access for about ten minutes after you attempt to download their video app. So I used my user agent override plug-in to make my netbook look like a smart phone to give it a whirl. The trick didn't work on Delta, so maybe Gogo has plugged that hole. Now they require side loading the app from their sandboxed Gogo domain.

Nonetheless, I noticed the mobile device user agent opened up a new Internet browsing option it didn't show before with my normal laptop user agent: T-Mobile users get free texting and calls during the flight, and also one hour free access to the full Internet. I'm a T-Mobile customer, but I left my cell phone at home. Besides, it's a flip phone that can't access the Internet anyway. Nonetheless, I wanted to see how far I could get without a cell phone. First, it asked me for my cell phone number. I assumed I would need to respond to a verification text or it would want some sort of app that verifies I'm accessing it from a T-Mobile device, but to my happy surprise this was all I needed to unlock a free hour of Internet on the flight. I was now able to catch up on my email, check the news headlines, send texts via Google Voice using my Linux netbook, all for no charge!

Unfortunately, I did not have other phone numbers to use after my hour expired, but it is very likely possible that it could open up a means to several hours of free Internet on Delta flights: just bring a list of T-Mobile numbers with you and, if your device is a laptop, a plug-in that makes your browser masquerade as a mobile device. You might need to clear your cookies and randomize your MAC address (macchanger for Linux users) if it has anything to monitor the device's authentication history. I'd love to hear from a *2600* reader what results you discover.

Don't have a list of T-Mobile numbers? Just go through your address book of phone numbers and plug them into `http://freecarrierlookup.com` to find out which ones are T-Mobile. If you don't want to use numbers from people you know, I've had luck finding T-Mobile numbers by just plugging in random phone numbers. Once I find a T-Mobile number, I can usually get several more by incrementing the last digit.

I don't know how long Delta and T-Mobile will offer this deal or what other airlines might have something similar, but take advantage of it while it lasts!



TELECOM INFORMER

by The Prophet

You wouldn't know that it's nearly spring here in the Pacific Northwest, given the sudden storm in Seattle that just dumped sleet all over the place. I'm in town again, working at my old Central Office in between my journeys to far-flung corners of the globe. It's an unusual role for me, but we're seeing a trend that is different than in years past: filthy CLECs are actually removing their equipment. There isn't much demand for POTS dial tone anymore, and CLECs are having a lot of trouble competing on broadband too. So, at least in some Central Offices, they are throwing in the towel. May as well not pay for a collocation cage that isn't really used.

In 2008, we deployed ADSL2+, which was pretty successful in driving filthy CLECs out of the ADSL business. It created so much interference in any cable with an ADSL pair that the CLECs didn't have a chance, especially because we used every trouble report as an opportunity to upsell to one of our own services. When we began the upgrade, we weren't actually required to provide any sort of line sharing or resale on our fiber-to-the-node (FTTN) network. Eventually, we were required to offer ADSL2+ to CLECs as a resale product, but by then the damage was already done. A few CLECs like sonic.net managed to hang around by becoming facilities-based, and FIOS also encroached into our service territory. For the most part, though, broadband competition consolidated down to a duopoly: The Phone Company and The Cable Company. Here in the U.S., we "enjoy" the fifth most expensive broadband in the developed world. The lack of competition keeps it that way and, for my part, I like it just fine. After all, people who work in industries with a lot of competition have to work really hard, and their pay tends to be a lot lower. As the manager, in addition to my fat paycheck, I get to decide how long I go for lunch - and today, that was three hours!

What a contrast to my recent visit to Myanmar, a rapidly developing country in southeast Asia. South of China, east of Bangladesh, and west of Thailand, Myanmar was run by the army for many years. My first visit to Myanmar was in 2013. I visited Kawthaung, opposite Ranong, Thailand, for a "visa run" while the military junta was still in charge (these days, Myanmar is a sort-of-democracy while a military junta rules Thailand - go figure). I met a local freelance tour guide named - of all things - Saddam. The guy was actually brilliant; he was only 20 years old and spoke seven different languages. After offering without success to connect me with all of the usual delights visitors to Kawthaung indulge in (drugs, prostitutes, and gambling, to name a few), I managed to convince him that I was really interested in learning how people use phones. So we went on a phone trip. I learned that there was only one mobile phone provider: MPT. SIM cards cost $200 plus an outrageously expensive service plan. Everyone in the local area used Thai networks instead, even though the signal from Thailand was weak and phones didn't work reliably indoors. And I learned that if you wanted to use the Internet, there was only one place in town, inside the one hotel in town. It operated at dial-up speed, was heavily censored, and cost over $5 per hour (a price that was astonishingly unaffordable to the local population). Most people couldn't afford smartphones, Wi-Fi was nonexistent, and Kawthaung was one of the more disconnected places I'd visited (although not to the extremes of Antarctica and North Korea).

Fast forward three years, and I landed in Yangon, the capital of Myanmar. I emerged from my Dragonair business class cabin into a nicer airport than any I've visited in the United States. There was free uncensored Wi-Fi. Everything was bright and modern. Well, I've seen this movie before, in Mumbai. As soon as I left the airport, I expected it would be like India - smog-choked, traffic-clogged, dilapidated infrastructure, and cows on the road. Nope. No cows on the road, hardly any traffic at night, wide boulevards. Don't get me wrong, it's a developing country, but Yangon was a massive contrast to the stray dogs and burning piles of trash I'd seen in Kawthaung a few years before. Not far from the Sule Pagoda, the driver dropped me off at my guest house.

My first two orders of business in the morning were changing money and obtaining a SIM card. I discovered to my annoyance that I had a problem with my money - I'd just grabbed a bunch of USD in $20 bills from the ATM in Seattle before I left. Unfortunately, in Myanmar, money changers are like kidnappers: they want only brand new unmarked bills. After several minutes of intense negotiations, they agreed to accept a few of my

$20 bills, handing me a black plastic shopping bag full of local currency.

I then proceeded next door to the cell phone shop. MPT, once the only mobile phone company in Myanmar, now has a lot of competition, and very competitive rates. SIM cards cost $1.50, and I bought a 4GB data plan for about $10, giving me access to a slow 3G network where I was able to attain maximum speeds of about 256Kbps (4G is deployed on a single tower in the country, near a popular mall in Yangon). Fortunately, tethering is allowed. I ended up needing to buy a lot more data packages because the availability of working Wi-Fi throughout the country is very limited. There is a huge amount of competition, but Internet access is very expensive and the Internet experience is very different for people in Myanmar than it is in most of the world.

Why is this? Myanmar's telecommunications landscape is almost the exact opposite of the U.S. Here in the U.S., we have limited local competition, but we're awash in international bandwidth for transit. Every major Internet backbone in the world has a point of presence here, and usually more than that - they have fiber. Since over half of the world's Internet traffic still originates, terminates, or transits through the U.S. (owing to the massive Internet data centers here hosting the majority of the world's most popular sites), telecommunications carriers need fast connectivity to our data centers. If you're in an American data center, you will generally have access to ridiculously fast, cheap connectivity to anywhere in the world. We just don't have that from home, where Internet service comes from a duopoly with little incentive to innovate.

Meanwhile, in Myanmar, Internet access is very slow and outrageously expensive because an international expansion project stalled for three years while the government changed in the middle of it. Fearing the uncertainty of the business environment, an international cable consortium led by Singtel waited out the change in government before resuming the project (and in all fairness, it wasn't clear until recently who they could even have made a deal with). There is only one small 100Gbps undersea fiber-optic cable serving the entire country, and it's running at full capacity; the new project will bring an additional 300Gpbs. By comparison, Facebook provides 160Gbps of uplink to every single rack in their data centers - and each data center has hundreds of racks!

The meager amount of bandwidth in Myanmar is not just bandwidth for Internet service, either. It's the available bandwidth for Internet, phones, corporate private networks, and anything else you can think of that runs over an international fiber optic network. More than 50 million people have to share it. This means that people almost exclusively experience the Internet using mobile phones and apps. It's so slow using a laptop that it's practically unusable; you can pretty much only use email and slowly browse the mobile versions of some websites. Remember night and weekend rates for phone calls? Myanmar actually has these for Internet; it's cheaper to go online in the middle of the night when demand is less.

Although there is currently no competition for international bandwidth, there is a ton of local "last mile" competition. Rather than only one mobile phone company operating in Myanmar, there are now three. And while the service is slow, it's usable, bringing Internet service to people who have never had it before. Internet companies are naturally doing everything they can to gain influence in the market. Lacking a concept of "net neutrality," web services pay mobile phone carriers to "zero rate" access to their services. For example, my MPT service offered a stripped-down version of Facebook for free (I couldn't see pictures or videos, only text). Telenor, another provider, offers "zero rated" WhatsApp and Line access, and Ooredoo offers free Facebook and mobile games.

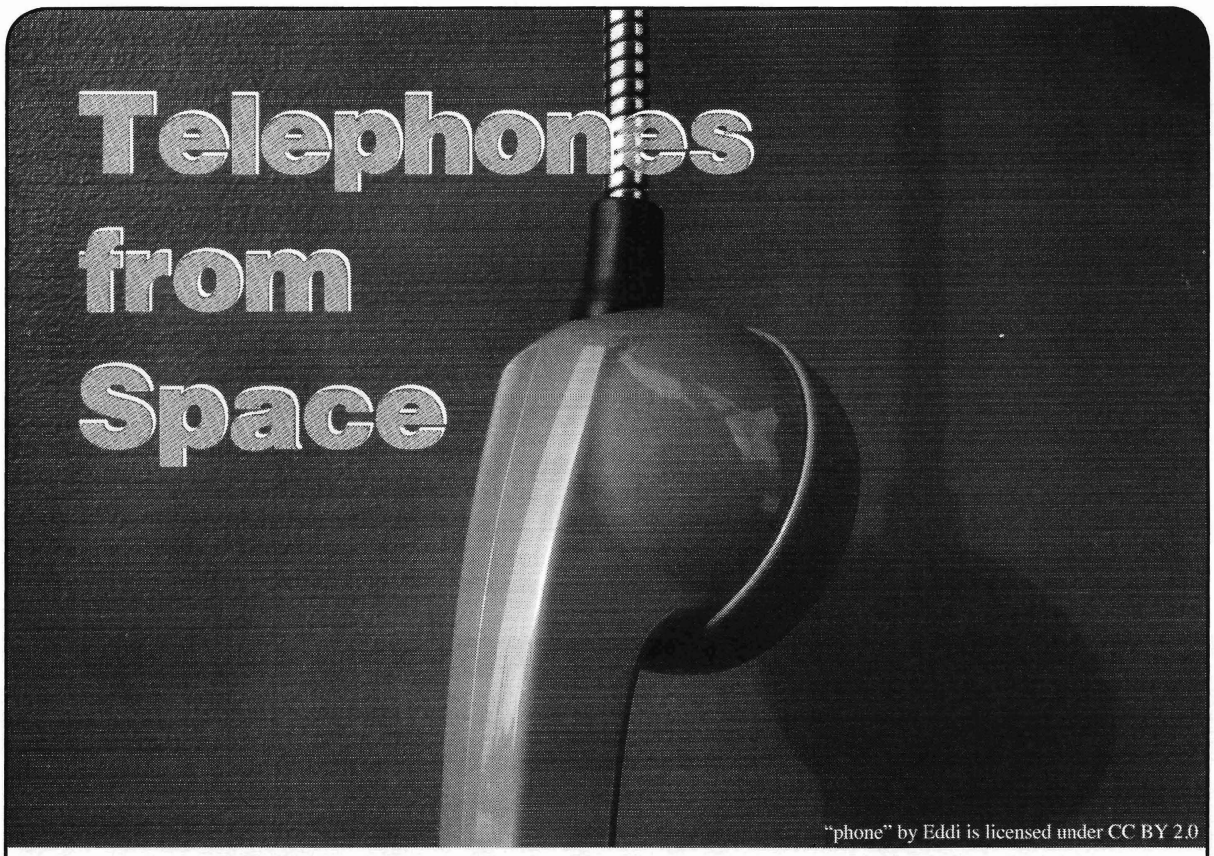
Competition isn't just limited to wireless carriers. There is competition with wireline carriers too, both formal and informal. I was surprised to discover the guest house I stayed in was equipped with fiber to the premises. While the equipment has the capacity to deliver Internet service at 1Gbps (along with VoIP phone and IPTV), the only affordable service is at 1Mbps. Another company, Myanmar Net, provides a hybrid wireline/wireless service. They run fiber to wireless access points sitting on top of utility poles throughout Yangon, then sell access to their Wi-Fi hotspots. There also appear to be informal ISPs in various neighborhoods. I spent a lot of time checking out utility poles in Yangon, and frequently spotted haphazardly strung Category 6 Ethernet cable. Given the very high cost of Internet access, it's not surprising that neighbors have found creative ways to share a single connection.

And with that, I'm back to removing DSLAMs, shutting off access cards, and taking the allergy medicine I obviously forgot. A... aaa..... dammit! Don't you hate it when you almost sneeze and can't? Stay safe out there, and I'll see you again in the summer.

References

Facebook data center network architecture - https://code.facebook.com/posts/➥360346274145943/introducing-data➥-center-fabric-the-next-generat➥ion-facebook-data-center-net➥work/

Sonic.net outside plant build - https://➥corp.sonic.net/ceo/2011/07/31/➥moving-outside-from-isp-to-osp/



by Dent
dentedfun@gmail.com
dentedfun@protonmail.ch

Modems, fax machines, old recordings, strange beeps, error messages, ancient answering machines, and pissed off operators. These are just a few of the amazing things I've encountered over the past few months. In this article I will talk about these things, how I found them and how you can find them yourself.

Some time in August, I picked up a payphone and called 1 800 200-1000. It rang for a good 30-60 seconds before I heard a loud screech from the speaker followed by silence. "Weird," I thought as I wrote it down in my blue notebook. This was followed by calling 1 800 201-1000, and then 1 800 202-1000. It wasn't long before I started finding all sorts of cool things. I compiled my full list and shared it with friends, only to find that these seemingly useless and unidentified numbers had a history of their own - even better, a community of their own.

This process is called *scanning*. It is also sometimes referred to as *hand scanning* or *exchange scanning*. To put it simply, it is the process of calling a range of numbers in sequential order with a goal of finding *something*. That *something* is up to you. Whether it be finding a strange recording or an elevator (yes, you can find elevators!), the things you write down and share are up to you. When I did my scans, I wrote down anything that I found to be cool. This included conferencing numbers, telecom companies, and pretty much anything I wanted to further investigate.

To start scanning, you only need a few things. Those things are:

1. What range you are scanning
2. A notebook and a pencil (or any way to log what you find)
3. A telephone!

To decide what range you are scanning, all you need to do is pick a phone number and a set of numbers that will increment after every call. In my previous example, it was:

```
1 800 NXX-1000
```

Keep in mind that the N is a number from 2 to 9 and the X is a number from 0 to 9. This means over a period of a few days (or a day if you're determined) you call around 800 different phone numbers. Within these many non-working numbers, you will find many cool things.

Below is an example of a scan I did in the 1 800 NXX-2600 range. Shortly after finishing this scan, I posted it to a phreaking forum under a different alias. You can still call most of these numbers by replacing "NXX" with a three digit number listed below.

```
229 - 2600 Magazine
250 - GBG Conferencing (requires 6-digit pin)
284 - Dungeon of Pain and Pleasure (lol)
288 - Vanderbilt University mailbox - "I'm sorry. Extension 26369 does
      ➥ not answer." (Callxpress VMS)
293 - AT&T Easy Reach 800 (requires "access code")
341 - Some phone number transaction line - provides instructions but no
      ➥ clear company or purpose
374 - Non Working Mobile Satellite Number
393 - "We're sorry. All circuits are busy now. Would you please try your
      ➥ call again later?"
423 - Rather rythmic beeps... playing forever...
428 - "We're sorry but this program has ended and no further calls are
      ➥ being taken. Thank you for calling."
455 - Instantly hangs up
493 - "We're sorry. All circuits are busy now. Would you please try your
      ➥ call again later?"
527 - Conference Center (requires access code)
533 - A very alarming number (badum tshhhh)
580 - Fax?
582 - Call Center
589 - Call Center (that likes to be called "Call Station")
594 - Voicemail of 404 330 9680
632 - Central Distribution System
658 - Fax
663 - Bell Aliant
674 - MCI (requires card number)
683 - "Sales auto attendant is not available..."
694 - Facebook Sales
716 - Numbers and beeps - strange but cool. (7-11 number)
723 - Same as 374
732 - Same as 428
832 - Silence
834 - Repair Escalation Line (they repair escalators I'm guessing?)
857 - Verizon Conferencing number that is not in use
861 - Disconnected number with TTY tones?
872 - Call Center
892 - Unregistered Brand800 Number
934 - Mobile Satellite Customer Not Answering
944 - Unregistered Brand800 Number
972 - Call Center
```

As you can see, there's a lot of cool stuff to find in plain sight. Even if you don't fully understand what you find, there is a puzzle to be solved, and therefore a story to be told.

I recommend recording particularly interesting numbers as well, in case they eventually claim a new purpose and what was once interesting is now just the voicemail of some guy named Bob.

Furthermore, sharing your scans with others is a great way to learn more about them. Without people like I-BaLL and ThoughtPhreaker, I would have never found or understood most of the numbers in this list. In the Links section of this article there are quite a few great places to share your scans with others.

Links

`http://www.binrev.com/forums/index.php?/forum/21-old-skool-phreaking/` - *Lots of threads all about scanning and a great community*

`https://www.youtube.com/watch?v=CQdv-NaFYrQ` - *A video I made about some of the numbers in this list as well as some others*

`http://textfiles.com/phreak/NUMBERS/` - *A collection of scans (mostly from the mid 1980s) put together by Jason Scott*

`http://oldskoolphreak.com/tfiles/` - *Lots of useful information about phreaking, scanning, and hacking*

Longing for the Past

by Nick

Here I am, writing a submission for *2600 Magazine*. I never thought I'd ever be writing a submission for *2600,* partly because I never have anything to talk about and my English writing skills really are awful!

Anyway, I'm 15 years old, live in London, and I am obsessed by telecommunications and computing history.

I own a ZX Spectrum+(48k). This is from 1982. I love to play the old games through the tape player and I also have a couple of old laptops pre-2002.

When I was around 13, I was looking "for places to telnet" and found this site called telehack.com. This is a site which gives you a "UNIX environment" and aims to recreate what the Internet was like back in the 1980s and 1990s. The aim of the game for the user is to take control of hosts by gaining root and downloading files from BBS. I still enjoy playing it.

From telehack I found out there was something called a BBS (Bulletin Board System) which was pretty much what everyone interested in computers used to talk to others on, as well as send mail and also download files.

In 2014, I bought a 56k modem so I could try dialing a few of these BBSes I found. Wow, did I have fun searching around! In 2014, there were only two dial-up BBSes left in the U.K.: Nostromo and The Arcade Acorn.

When I last checked (about a month ago), The Arcade Acorn was no longer around, however Nostromo still is. I know BBSes are accessible through telnet, but that's no fun! The reason I dial these instead of "telnetting" in is because it makes me feel nostalgic (I really wish I was born in the sixties. By the eighties I would be old enough to afford a computer and a modem, and play around with all this stuff back then).

Eventually, I got a little bored of the BBSes in the U.K., so I decided to look for other dial-up ones. I found a large list (Synchronet) of dial-up BBSes - wow, I was happy, but problem: they were all in the U.S.

I managed to find a way to make a "cheap" call to the U.S. I dialed most of the BBSes on that list until my dad asked me why we had such a big phone bill of 0844 numbers.

I told him how I used 0844 numbers to get a "cheap" call to the U.S. I told him that on the site it was 1p a min which didn't seem such a big deal to me, but what I didn't realize was that BT (British Telecom) charged 33p to access an 0844 number! He was a bit pissed off for a while, but whatever. You can't blame me, I was only 13!

Eventually, I got bored of dialing BBSes and I just stopped after about a year of exploring various boards and dial-up numbers.

Only recently has my interest started again as I have read the *2600* 1984 *Hacker Digest,* Volume 1.

It's not so much the BBSes anymore or even the modem that amuses me; it's the phreaking. Back when I was interested in BBSes and modems, I had an idea as to what phreaking was, but not to the extent which I understand it now.

I don't think you understand how much I would love to dial through different exchanges, scan different 1-800 numbers, and play 2600 hertz through a phonebox to get a free long distance call. It must've been so fun!

I watched the movie *Hackers* and never really understood it until I watched it again a few weeks ago. It's sick! I always understood the movie *War Games* - it's a great movie too!

I was surfing the net the other night, trying to find out if there were any exchanges that were "phreakable" and unfortunately the last one closed down just over ten years ago.

However, what I did find is something that really interests me: Project MF.

Project MF is a number you can dial which acts as a "phreakable" exchange. You need a blue box whether it be physical, a computer program, or a smartphone app.

You can play 2600 hertz to seize the line, use "KP - number - ST," and it takes you to its extension numbers that are programmed in.

This is only an American number, which is annoying because I have to dial a cheap call to the USA number first, then dial the Project MF number (+1-630-485-2995). If anyone lives in the U.K. and wishes to dial the US for free, use 0333-555-3872. This is an 03 number and, as you know (if you live in the U.K.) 01/02/03 numbers are free to call as they are geographical numbers.

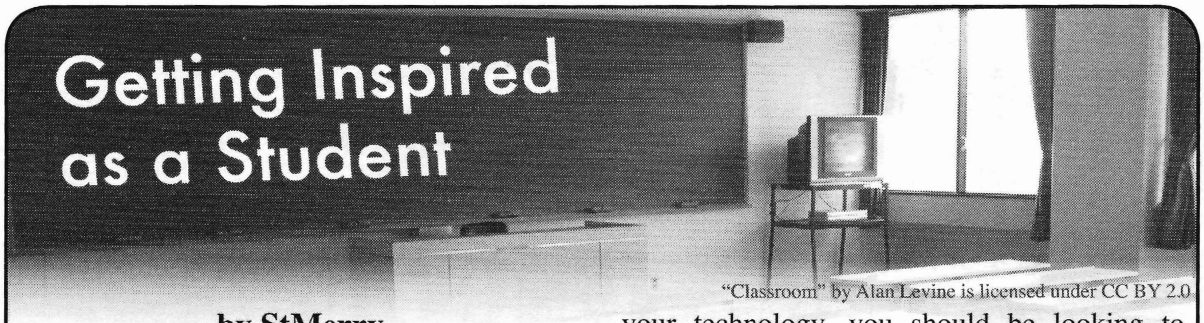
It's amazing. It might be outdated to you guys that grew up in the 1980s and 1990s. You've had first hand experience. But this really does interest me.

I was 11 when I sent my first fax. I kept on sending them to my dad's office, another reason for him to get pissed off.

Man, I wish I could go back to the past and experience all of this cool stuff, even though I have an iPhone and a Windows 10 PC, which obviously were not around 20 to 30 years ago.

I would rather be in the past than where I am now.

Getting Inspired as a Student



"Classroom" by Alan Levine is licensed under CC BY 2.0

by StMerry

Last November in London, information security professionals and aspiring students alike gathered at Black Hat Europe 2016, the most respected conference in the industry. Briefings included presenters from all over the world, from the U.S. to Russia and China, on a wide range of topics such as mobile hacking, cryptography, data forensics and incident response, exploit development, malware defense and offense, web appsec, car penetration-testing, and many more. I was thrilled with the idea of mixing up with what to me represent some of the smartest minds of this century, all for the love of hacking and sharing of knowledge. I was especially glad to be there after having been offered one of the hundred studentships. However, I left the conference with a wee bit of a bitter taste after visiting the business hall, which is basically the vendors area. And there were two reasons for that.

The business hall was relatively small but packed, with vendors of different backgrounds organized next to each other. In between the talks, it was possible to roam for a while and meet companies present for the day, which seemed like an interesting opportunity to get to know the latest in terms of technology and solutions against so called "cyber-attacks." I was quickly disappointed however, to see that the vast majority of the people representing these companies had no technical background whatsoever, and mostly learned their sales speech. Now, most of you who have been to Black Hat won't be too surprised, however what bothered me the most was the fact that these salesmen and women had no real interest in engaging with us. As a matter of fact, we quickly felt unwelcome as they looked down on us, most likely understanding that we were not ones to strike deals with. After all, we were simply a group of students with an interest in and questions on how their technology actually works.

Why is it that we felt so ignored? If a group of passionate security graduates comes forward to engage with your company and learn about your technology, you should be looking to share - to a minimal extent - relevant knowledge about it. You should be looking to inspire us, make us want to research more around your solution, which could in turn possibly even result in us improving it in the future, however ambitious this may sound. Instead, you have made the decision to not waste your time with us because you sent someone with one thing in mind: attracting customers and growing sales, forgetting everything and everyone around you.

Another thing that bothered me, again, after roaming between vendors, was the high interest around applying Artificial Intelligence (AI) solutions, such as Machine Learning (ML). I have nothing against this technology. In fact, I have researched and applied it, but it certainly felt like those vendors simply were using it more as a buzzword than an actual solution. I ended up playing a game, which was asking each of those companies the following question: "What makes you stand out from the other hundred companies present today that are selling similar solutions?" The answer: "We use the Cloud!" In other words, either nothing, or they did not have enough technical knowledge to back it up. I do believe we have a lot to learn from applying AI and ML solutions properly and effectively, but this is not and will never be a magic solution against breaches. There will always be a way around defenses, as there always have been. And claiming that this suddenly will change because we can recognize patterns more effectively (which in essence is what ML is used for) is way too optimistic in my opinion. One of these companies was even claiming to be able to run a full penetration test in under four and a half minutes.

Now don't get me wrong. I met a number of interesting people and companies at Black Hat Europe this year, but I do feel like there was a need to highlight these points, especially around how I felt as a research student, trying to get inspired and engage as much as I possibly could. Overall however, it was a fantastic conference once again, and I am definitely looking forward to next year.

by Ry0ki

2015 and 2016 have been interesting in politics, referendum votes, and elections around the globe. Increasingly, the Internet is used in political elections from VoIP, social media, websites, email, news, and search engines. We'll focus on Google auto-fill suggestion bombing results. A friend gave me a taste of what she had found. I travel a lot, get bored waiting for flights, and looked deeper.

Search engine manipulation is making search engine ranking, auto-fill, or other results return what you want. This can be done through manipulation of algorithm results and a bevy of other techniques. One famous example involved the Google bombing of a previous 2004 Republican presidential candidate, Rick Santorum. Just search "Santorum" on Google....

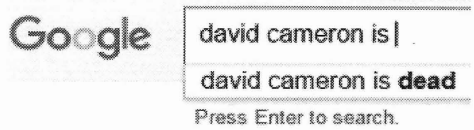
Let's look at examples from the first half of 2016. I broke it down by country using roughly the same search terms, using country-specific language where applicable. Some of the results I noticed changed over time. I was filter bubbled by Google so results may vary. (Bubbling is when Google returns search results based on a number of variants including which country version used, what computer, phone, cookies you have installed, etc.)

I used candidates for important offices I knew of at the time or of importance. I couldn't translate everything correctly, please send in corrections to the *2600* Letters to the Editor. I'm very curious. Hopefully this will encourage you to go deeper as well.

Search term: "first name", "surname", plus "is" using English and, where applicable, German.

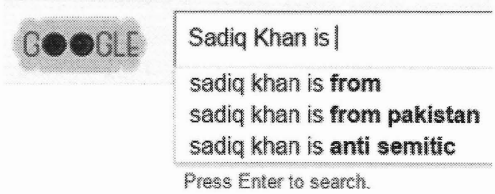
United Kingdom

David Cameron - Prime Minister (at time of search)

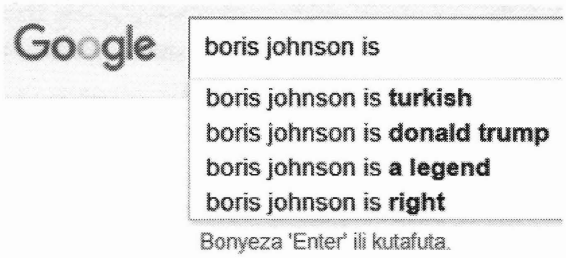


I got the same results throughout 2016. Recently, the U.K. Works and Pensions department has been declaring a lot of live people dead and cutting off benefits. Mr. Cameron better be careful or he might lose benefits himself with search results like this.

Sadiq Khan - Mayor of London, recently elected.

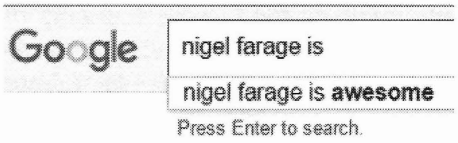


Boris Johnson - previous Mayor of London,
before the Mayoral election compared to a week before the Brexit vote 2016.

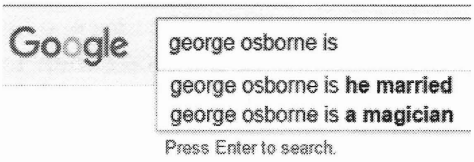


I myself have seen similarities between Borris and The Donald. Interesting....

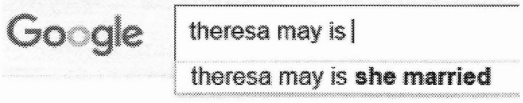
Nigel Farage - leader of the UKIP party, Far Right



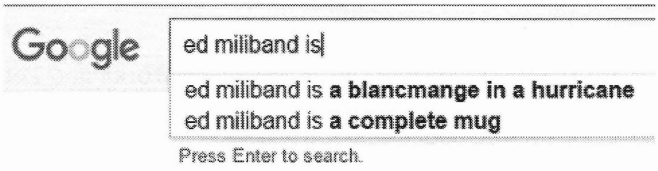
George Osborne - Chancellor of the Exchequer



Theresa May - Home Secretary (at time of search)

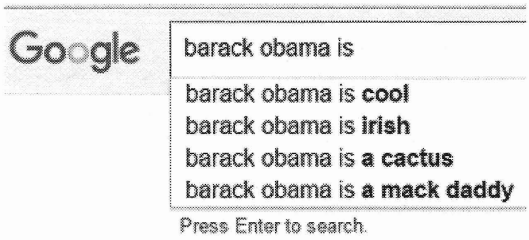


Ed Miliband - Leader of the Labour Party (at time of search)



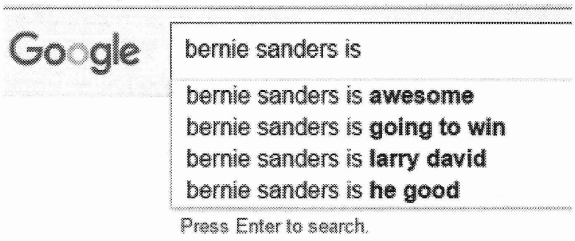
United States

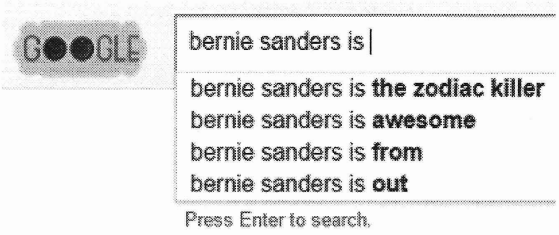
Barack Obama - President



Mack Daddy, much more positive results vs. Mr. Cameron.

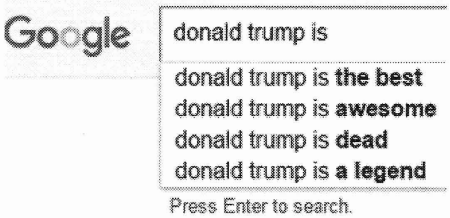
Bernie Sanders - Democratic presidential candidate.
The first search was performed in April 2016 while in the U.K.
The second one was performed in June 2016 while in the Netherlands.

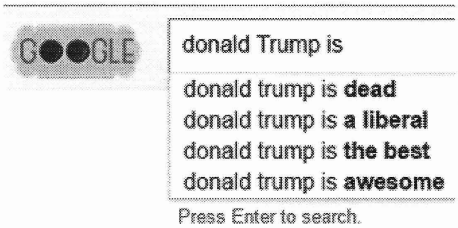




When Bernie had a more optimistic outlook, the auto-fill was much more favorable versus later on in the campaign.

Donald Trump - Republican presidential candidate.
The first search was performed in April 2016 while in the U.K.
The second one was performed in June 2016 while in the Netherlands.





(Continued on page 54)

The Inner Circle... Part One

"TRUMP","DONALD","J","","721","","PH","","5 AVENUE ","","NEW YORK","10022",
"1002","","","","","19460614","M","REP","","31","46","0","NEW YORK","","12"
,"28","73","20160419",""," ","","","YY0089904","19870701","MAIL","N","Y",
"ACTIVE","","","","NY000000000037517720","20160419 PP;20141104 GE;20131105
GE;20130910 PR;20121106 GE;20101102 GE;20100914 PR;20091103 GE;20081104
GE;General Election 2006;General Election 2005;General Election 2004"

"TRUMP","MELANIA","","","721","","66N","","5 AVENUE ","","MANHATTAN",
"10022","","","","","","19700426","F","REP","","31","46","","NEW YORK","",
"12","28","73","20160419",""," ","","","306293451","20061013",
"MAIL","N","Y","ACTIVE","","","","NY000000000037469080","20160419
PP;20121106 GE;20101102 GE;20081104 GE;General Election 2006"

"TRUMP","DONALD","J","JR","425","","12CD","","EAST 58 STREET ","",
"MANHATTAN","10022","","725 FIFTH AVENUE","NEW YORK, NY
10022","","","19771231","M","REP","","31","38","0","MANHA
TTAN","","12","28","73","20160419",""," ","","","306090388","20030825",
"MAIL","N","Y","ACTIVE","","","","NY000000000037414449","20160419 PP;20141104
GE;20131105 GE;20121106 GE;20101102 GE;20091103 GE;20081104 GE;20080205 PP"

"TRUMP","VANESSA","K","","425","","12 C AND D","","EAST 58 STREET ","","MANH
ATTAN","10022","","","","","","19771218","F","BLK","","31","38","0","MANHA
TTAN","","12","28","73","20141104",""," ","","","303082105","19960729","MAIL
","N","Y","ACTIVE","","","","NY000000000037832260","20141104 GE;20131105
GE;20121106 GE;20081104 GE;General Election 2004;General Election 2002"

"TRUMP","IVANKA","M","","502","","28","","PARK AVENUE ","","NEW YORK
","10022","1002","","","","","","19811030","F","REP","","31","46","0",
"NEW YORK","","12","28","73","20141104","","31","","","306289305","2006
1013","MAIL","N","Y","ACTIVE","","","","NY000000000037467270","20141104
GE;20131105 GE;20121106 GE;20091103 GE;20081104 GE;General Election 2006"

"KUSHNER","JARED","C","","502","","PH28","","PARK AVENUE
","","Manhattan","10022","","","","","","","19810110","F","BLK","
","31","46","0","Manhattan","","12","28","73","20141104","","
","","","410701149","20091124","MAIL","N","Y","ACTIVE","","","",""
,"NY000000000051749029","20141104 GE;20131105 GE;20121106 GE;20101102 GE"

"TRUMP","ERIC","F","","100","","14D","","CENTRAL PARK S ","","NEW YORK","1
0019","1001","","","","","","19840106","M","REP","","31","91","0","NEW YORK",
"","12","28","75","20141104",""," ","","","410076901","20080109","MAIL","
N","Y","ACTIVE","","","","NY000000000050252090","20141104 GE;20121106 GE"

"TRUMP","LARA","YUNASKA","","100","","14D","","CENTRAL PARK SOUTH ","","NEW
YORK","10019","1001","","","","","","19821012","F","REP","","31","91","0","NEW
YORK","","12","28","75","20141104","","31","","","410618753","20090528","MAIL
","N","Y","ACTIVE","","","","NY000000000051538628","20141104 GE;20121106 GE"

"TRUMP","TIFFANY","A","","167","","36B","","EAST 61 STREET ","","NEW
YORK","10065","1006","","","","","","19931013","F","REP","","31","50
","","NEW YORK","","12","28","73","","","99","3925 WALNUT STREET
APT 304 PHILADELPHIA 19104","","412584527","20161013","MAIL
","N","Y","ACTIVE","","","","NY000000000055958709",""

"BARRY","MARYANNE","T","","1050","","15F","","5 AVENUE ","","NEW YORK","100
28","1002","","","","","19370405","F","BLK","","31","80","0","NEW YORK",""
,"12","28","73","20121106","","99","5 ISLAND TRAIL SPARTA","","304411563","
19990803","MAIL","N","Y","ACTIVE","","","","NY000000000038023480","20121106
GE;20091103 GE;20090929 RO;20090915 PR;20081104 GE;20080909 PR;20080205
PP;20071106 GE;General Election 2006;City Primary Election 2006;General
Election 2005;City Primary Election 2005;General Election 2004;Primary
Election 2004;General Election 2003;General Election 2002"

"BANNON","STEPHEN","K","","32","","2 NORTH","","WEST 40 STREET ","","NEW
YORK","10018","1001","","","","","19531127","M","REP","","31","58","",
"NEW YORK","","12","27","75","",""," ","","","412624254","20161014","MAIL
","N","Y","ACTIVE","","","","NY000000000056060263",""

"CONWAY","KELLYANNE","E","","845","","80D","","UNITED NATIONS PLAZA
","","MANHATTAN","10017","","","","","","","19670120","F","CON","","31","16"
,"","NEW YORK","","12","28","73","20071106","","99","1475 CARRINGTON RIDGE
LANE VIENNA VA","","306274255","20061004","MAIL","N","Y","PURGED","OTHER",
"","20130311","NY000000000037462642","20071106 GE;General Election 2006"

"CONWAY","GEORGE","T","","845","","80D","","UNITED NATIONS PLAZA ","","MANH
ATTAN","10017","","","","","","","19630902","M","CON","","31","9","0","MANH
ATTAN","04","14","26","73","20071106","","99","1475 CARRINGTON RIDGE LN
VIENNA VA","","306267743","20060914","MAIL","N","Y","PURGED","MOVED","20090
530","20090530","NY000000000037460152","20071106 GE;General Election 2006"

"POWELL","DINA","H","","181","","APT 15C","","EAST 90 STREET
","","NEW YORK","10128","","","","","","","19730623","F","REP","","31
","90","0","Manhattan","","12","28","73","20160419","","10","3525
N. PINWIDDLE ST, VA","","410301595","20080828","MAIL","N","Y",
"ACTIVE","","","","NY000000000050829833","20160419 PP;20141104
GE;20131105 GE;20121106 GE;20101102 GE;20100914 PR;20081104 GE"

"MNUCHIN","STEVEN","T","","740","","8A","","PARK AVENUE ","","MANHATTAN"
,"10021","","","","","","","19621221","M","REP","","31","61","","NEW YORK",
"","12","28","73","20081104",""," ","","","302765642","19951227","MAIL
","N","Y","ACTIVE","","","","NY000000000037796798","20081104
GE;General Election 2005;General Election 2004"

"FRIEDMAN","DAVID","M","","12","","","","WOOD LN","S","
WOODMERE","11598","","","","","","","19580808","M","DEM","
","30","27","4","HEM","20","4","9","20","20141104","","
","","","03853526","19961009","LOCALREG","N","Y","ACTIVE","","","",""
,"NY000000000038759635","2014 GENERAL ELECTION;2012 GENERAL ELECTION;2010
GENERAL ELECTION;2008 GENERAL ELECTION;2004 GENERAL ELECTION"

"FEINBERG","STEPHEN","A","","36","","","","EAST 67 STREET ","","NEW YORK","
10065","","","","","","","19600329","M","REP","","31","56","","NEW YORK","","1
2","28","73","20160419",""," ","","","304705518","20000620","MAIL","N","Y"
,"ACTIVE","","","","NY000000000038080223","20160419 PP;20141104 GE;20121106
GE;20101102 GE;20081104 GE;General Election 2006;General Election 2004"

"BENDER","DONALD","","","5","","","","WOODTREE DR","","WOODBURY
","11797","","","","","","","19571208","M","DEM","","30","27","16"
,"OB","13","3","5","13","20151103",""," ","","","03542480","19920708","LOCA
LREG","N","Y","ACTIVE","","","","NY000000000039239203","2015 GENERAL
ELECTION;2014 GENERAL ELECTION;2010 GENERAL ELECTION;2009 GENERAL
ELECTION;2008 GENERAL ELECTION;2007 GENERAL ELECTION;2006 GENERAL
ELECTION;2005 GENERAL ELECTION;2004 GENERAL ELECTION;2002 GENERAL ELECTION"

```
"WEISSELBERG","ALLEN","H","","1108","","","","MC LEAN AVE"
,"","WANTAGH","11793","","","","","","19470815","M","DEM",
"","30","12","13","HEM","14","2","6","14","20041102","","
",","","02850918","19821001","LOCALREG","N","Y","PURGED","MOV
ED","","","NY000000000038654325","2004 GENERAL ELECTION"

"WEISSELBERG","ALLEN","H","","140","","2102","","RIVERSIDE BOULEVARD
",","","NEW YORK","10069","1006","","","","","19470815","M","REP"
,"","31","45","","NEW YORK","","10","27","67","","","30","1108
MCLEAN AVENUE WANTAAGHN.Y 11793","","412321740","20160510","MAIL
","N","Y","ACTIVE","","","","NY000000000055444808",""

"BORNSTEIN","HAROLD","","","101","","","","EAST   78 STREET ",","","MANHA
TTAN","10075","","","","","","19470326","M","REP","","31","63","","NEW
YORK","","14","26","73","","","  ",","","N1071155","19820101","LOCALR
EG","N","Y","PURGED","MOVED","","20120127","NY000000000038018988",""

"BORNSTEIN","HAROLD","N","","19","","","","BOULDER BROOK RD","","SCAR
SDALE","10583","","","","","","19470326","M","BLK","","60","18","5","
SCRD","","16","35","88","20161108","","  ",","","97279612","20081004","LOCA
LREG","N","Y","ACTIVE","","","","NY000000000050961918","GENERAL
2016;GENERAL 2014;GENERAL 2012;GENERAL 2010;GENERAL 2008"

"EPSHTEYN","BORIS","","","155","","APT 7H","","WEST 21 STREET ","","NEW
YORK","10011","","","","","","19820814","M","REP","","31","17","0","Manha
ttan","","12","27","75","20160419","","  ",","","410073286","20080111","MAIL
","N","Y","ACTIVE","","","","NY000000000050245510","20160419
PP;20121106 GE;20101102 GE;20081104 GE;20080205 PP"

"GIULIANI","RUDOLPH","W","","45","","","","EAST 66 STREET
",","","NEW YORK","10065","1006","","","","","19440528","M","REP
","","31","56","0","NEW YORK","","12","28","73","20160419",""
,"  ",","","302322805","19840101","LOCALREG","N","Y","ACTIVE","","","
","NY000000000037749986","20160419 PP;20151103 GE;20141104 GE;20131105
GE;20130910 PR;20121106 GE;20120626 PR;20120424 PP;20111108 GE;20110913
SP;20101102 GE;20100914 PR;20091103 GE;20081104 GE;20080205 PP;20071106
GE;General Election 2006;City Primary Election 2006;General Election
2005;General Election 2004;General Election 2003;General Election 2002"

"STONE","ROGER","J","","55","","25L","","WEST 25 STREET
",","","MANHATTAN","10010","","","","","","19520827","M","CON","
","31","29","0","MANHATTAN","","12","28","75","20021105","","
",","","304848953","20001010","MAIL","N","Y","INACTIVE","MAILCHECK
","20130312","","NY000000000038115915","General Election 2002"

"MURDOCH","KEITH","R","","23","","PH","","EAST 22 STREET ","","NEW YORK
","10010","1001","","","","","19310311","M","BLK","","31","30","0",
"NEW YORK","","12","28","75","20121106","","31","","","304573235","2000
0127","MAIL","N","Y","ACTIVE","","","","NY000000000038055480","20121106
GE;20101102 GE;General Election 2004;General Election 2002"

"AILES","ROGER","E","","44","","","","BEVERLY WARREN RD ","","GARRISON","105
24","4409","PO BOX 353","GARRISON, NY 10524-0353","","","19400515","M","REP"
,"","40","11","1","PHILIPSTOWN","000","18","41","95","20161108","","99","218
TRUMAN DR CRESSKILL NJ 07626","AILES ROGER E","30015932","20120207","CB
OE","N","Y","ACTIVE","","","","NY000000000052569291","General Election
2016;General Election 2015;General Election 2013;General Election 2012"
```

"OREILLY","WILLIAM","J","","33","","","","SHORE DR","","MANHASSE
T","11030","","","","","","19490910","M","IND","","30","57","9"
,"NH","16","3","7","16","20151103",""," ","","","03699383","19940919","LOCA
LREG","N","Y","ACTIVE","","","","NY0000000000039011259","2015 GENERAL
ELECTION;2014 GENERAL ELECTION;2013 GENERAL ELECTION;2012 GENERAL
ELECTION;2011 GENERAL ELECTION;2010 GENERAL ELECTION;2009 GENERAL ELECTION;2008
GENERAL ELECTION;2007 GENERAL ELECTION;SPECIAL ELECTION 7TH SD;2006 GENERAL
ELECTION;2005 GENERAL ELECTION;2004 GENERAL ELECTION;2002 GENERAL ELECTION"

"HANNITY","SEAN","","","27","","","","SEACREST DR","","LLOYD
HARBOR","11743","9765","406 CENTER ISLAND RD","CENTRE ISLAND
NY 11771","","","19611230","M","REP","","52","119","18","HUNTIN
GTON","","3","5","10","20081104",""," ","","","09671646","20000322","CBOE","N
","Y","PURGED","MOVED","","20110404","NY0000000000009956890","General Election,
2008;General Election, 2006;General Election, 2004;General Election, 2002"

"HANNITY","SEAN","","","406","","","","CENTRE ISLAND RD","","OYSTER
BAY","11771","","","","","","19611230","M","CON","","30","6","18"
,"OB","13","3","5","13","20141104",""," ","","","99442620","20091222","LOCA
LREG","N","Y","ACTIVE","","","","NY0000000000009956890","2014 GENERAL
ELECTION;2013 GENERAL ELECTION;2012 GENERAL ELECTION;General Election,
2008;General Election, 2006;General Election, 2004;General Election, 2002"

"RUDDY","CHRISTOPHER","W","","93","","","","CORNELL ST","","WILLISTON
PARK","11596","","","","","","19650128","M","REP","","30","33","9"
,"NH","19","3","7","19","",""," ","","","02862983","19830225","LOCA
LREG","N","Y","PURGED","MOVED","","","NY0000000000054055712",""

"PAGE","CARTER","","","6","","","","GASKIN RD","","POUGHKEEPSIE","1
2601","5015","","","","","19710603","M","REP","","14","3","8","City
Poughkeepsie","004","22","41","100","",""," ","","","R123260","19890316",
"CBOE","N","Y","PURGED","MOVED","","20080124","NY0000000000022057599",""

"PAGE","CARTER","W","","10","","46F","","BARCLAY STREET ","","Manha
ttan","10007","","","","","","19710603","M","REP","","31","3","0","
Manhattan","01","8","25","66","20081104","","14","6 GASKIN RD POUGH
NY","","410059215","20071231","MAIL","N","Y","PURGED","MOVED","",
"20090711","NY0000000000022057599","20081104 GE;20080205 PP"

"PAGE","CARTER","","","6","","","","GASKIN RD ","","POUGHKEEPSI
E","12601","","C/O GLOBAL ENERGY CAPITAL LLC","590 MADISON AVE
21ST FLOOR","NEW YORK, NY 10022","","19710603","M","REP","","
14","2","8","City Poughkeepsie","004","18","41","104","","","
","","","10164927","20161024","CBOE","N","Y","ACTI
VE","","","","NY0000000000056129575",""

"NUNBERG","SAMUEL","D","","535","","2 J","","EAST 86 STREET ","","MANHATTAN","1
0028","","","","","","","19810621","M","REP","","31","70","","NEW YORK","","12","2
8","76","20141104",""," ","","","304738177","20000803","MAIL","N","Y","ACTIVE
","","","","NY0000000000038086818","20141104 GE;20131105 GE;20130910 PR;20121106
GE;20120626 PR;20120424 PP;20101102 GE;20100914 PR;20091103 GE;20081104
GE;20080205 PP;20071106 GE;General Election 2006;City Primary Election
2006;General Election 2005;General Election 2004;General Election 2003"

"COHEN","MICHAEL","D","","502","","10A","","PARK AVENUE ","","Manhatta
n","10022","","","","","","19660825","M","DEM","","31","46","0","Manha
ttan","","12","28","73","20121106",""," ","","","410969372","20111222","MAIL
","N","Y","ACTIVE","","","","NY0000000000052521993","20121106 GE"

"COHEN","MICHAEL","D","","120","","R12E","","EAST   87 STREET ","","MANH
ATTAN","10128","","","","","","19660825","M","DEM","","31","83","","NEW
YORK","","14","26","73","",""," ","","","301707408","20001107","MAIL
","N","Y","PURGED","OTHER","","20090328","NY0000000000037706562",""

The Hacker Perspective

by Jack Beltane

Trust is a powerful thing, and it starts with nothing. As children, we are taught not to talk to strangers, but we see our parents do it all the time. Children see that, to adults, trust starts with a handshake. What children don't understand is how much information is packed into a handshake: the firmness of the grip, how sweaty the palms are, if the smile on the lips is mirrored in the eyes. As children, we don't fully understand how a simple handshake can help determine trust for our parents.

Computers do the same thing before they'll talk to each other, offering an introductory handshake and weighing the response. But computers are binary and their users, like children, don't understand what the handshake does - or doesn't do. Computers don't read subtle signs and cues in a handshake to help determine a level of trust. Computers make a set series of snap judgments and return a 1 or 0. Trust/not. That's why it's so easy to fool a computer and spoof false trust with a handshake. In humans, using the subtle cues in a handshake to spoof trust is an art reserved for the very best salespeople and scam artists who can bilk an unsuspecting rube of thousands or millions of dollars.

In an effort to combat human spoofing, we don't fully trust anyone, even with a handshake. Trust has to be earned. Trust has to be maintained. Trust can never be rebuilt. Machines trust far too easily in order to avoid bogging down users with passwords and credentials checks multiple times in a single session. The problem is, most humans believe that the binary line of trust used by computers keeps them safe. Humans forget that it's still up to us, not the machines, to interpret the subtle signs and cues in every handshake and, from there, go beyond the handshake and build a complete trust profile.

I've always looked sketchy: earrings, tattoos, mohawks, black nail polish. Now I'm middle aged and I've dialed back the overt rebellion, but I've kept the earrings, and the tattoos aren't going anywhere. At parent-teacher conferences, I still catch sidelong glances from soccer moms and salesman dads. They figure they don't need a handshake to determine that my kids should stay away from their kids. What my years of overt rebellion have taught me is simple: Perception is the first human filter, and it's up to us to change - or prove - the perception of another, starting with a handshake.

Most humans are polite and logical, which allows us to initiate a handshake and, from there, if the handshake returns a 1, go beyond it to establish if the perception was correct or may need to be adjusted: An assessment taking nanoseconds of subconscious processing that reaches the brain as a gut feeling. Salespeople are well versed in the gut feeling. Nobody trusts a salesperson - that perception is set in stone. However, salespeople will tell you that perception is easy to overcome with a trustworthy handshake. The last 30 years have taught me the same thing: words and actions speak louder than perception.

Computers do not benefit from first impressions and gut feelings. First contact determines 1 or 0. Trust/not. They cannot go beyond the handshake. Computers grant access and establish trust either one-way (the domain trusts the user logged in, for example) or two-way (the user's machine and the domain both establish trust with each other). Human trust could be similarly distinguished, and access granted in response, but instances of one-way trust among humans are reserved most obviously for the shyster-rube relationship. More subtle is how corporations view coders.

Most corporations handle employee relationships, especially with employees who have a proficiency for computers and coding, with a one-way trust, expecting their employees to trust them even as they do not truly trust their employees. Most employees naively believe it's a two-way trust: they trust the employer and they believe their employer trusts them. Employees assume that the interview and eventual hiring was handshake, perception, credential checks, and acceptance in one neat bundle, establishing a solid two-way trust.

The first "career" job I had for a faceless corporation didn't bother to go beyond the handshake when they learned of a script I'd written. The script wasn't anything amazing, which is why it never occurred to me to clear it with my superiors. At that point, I was suffering under the

delusion of a two-way trust. I wrote the script for the same reason most hacks are developed: to make life easier and processes more efficient. I had to open, paginate, and number 400-plus separate Word files so they could be combined into a single, consecutively numbered file for two distinct volumes. I'm leaving out a lot of details about why this massive inefficiency existed (it took me about 40 mind-numbing hours to do it their way), but I was inspired to let my machine do its job and open, paginate, and number the files for me. It took the script about two minutes to accomplish what took me a week. I wish I was exaggerating.

By way of thanks, I got written up and my next three reviews mentioned my infraction. Big Company One had a whole department for scripting, it turned out, and they didn't trust anyone else to write code. The Scripting Department was overworked, most likely underpaid, and even more likely had the scripts they developed overseen and changed by ignorant middle managers. It was how Big Company One dealt with the issue of gray-hats - coders who had yet to prove if their intentions were black- or white-hat - as if locking all the tigers in a cage negated any possibility of danger.

To be clear, I've never been a black-hat user. The most malicious thing I've done with computers was back in high school, when I finished my computer assignment early and spent the rest of the class poking around in the settings and configuration files on my workstation. When I left at the bell, all the machines in the lab had pink-on-yellow displays (this was the 8-bit era) and their keyboards set to Dvorak, rendering the hot keys for settings useless unless you knew the Dvorak keyboard layout. I got called out of my next class to fix it, but I didn't get in any trouble and, to this day, I don't know if they asked for my help because they knew I'd done it or because they figured I could fix it. If he'd had the lingo, my teacher would have viewed me as a gray-hat. After that, I did what I could to prove he could trust me.

Because of the red tape, the Scripting Department at Big Company One was massively inefficient, and it didn't take long for my reputation to spread as the guy who could rewrite a script that didn't work, or help someone who needed a script immediately to meet a deadline that the Scripting Department wouldn't be able to beat. That's when I realized the perception of my employers wasn't wrong; I was a gray-hat and, for all they knew, possibly a black-hat. I had to work off the books by word of mouth. If someone sent me an email, I dutifully responded that they had to go through the Scripting Department, then walked over to their cube, swore them to secrecy, and asked how I could help. Scripts were delivered on floppy disks - I knew the Company was watching. They read our emails, sniffed our network traffic, and used our badges to triangulate where in the building we were, when we got there, and how long we stayed. It's hard to do anything at work without your employer knowing or being able to find out.

To Big Company One, I was a hacker who'd been caught once, and the fact that I kept doing it put me on the wrong side of the rules. I didn't have a chance to go beyond the handshake and prove the actual color of my intentions to them, but to myself and other employees, I saved jobs with scripts that made unrealistic deadlines realistic. My peers saw and accepted that gray area, but corporations behave more like machines and to them the question was binary: 1 or 0. Trust/not. White/black.

The inherent distrust of Big Company One made me less trustworthy, not more compliant. The way the company viewed me was directly responsible for shading my hat to gray, maybe even charcoal. They created a perception and relied on a handshake that they refused to look beyond. Ironically, their distrust motivated me to work under the counter. It forced me to learn ways of communicating and passing data without leaving footprints behind, and it proved to me that I was working for the wrong people. I didn't want to hide my skills, lie, and cover my tracks just to help fellow employees work more efficiently. It didn't feel right.

My current job is not like most corporations, which is why I'm closing in on ten years with them. It's big, but not faceless, and it assumed I was a white-hat from my first day. It trusted its own interview processes as a handshake to root out nefarious employees, and it used other employees who had proved themselves trustworthy to go beyond that handshake. Perception - the earrings and tattoos - didn't even figure into it.

Not long after I'd been hired, my team lead asked about the computer languages I'd listed on my resume and wondered if I could look at a VBScript a previous employee had written. It was used to run about 200 unique shell processes, one after the other, but it would crash randomly with no way of telling how many of the 200 processes had been completed, and whether or not they had completed successfully. I had not been hired to perform any kind of scripting, and they just wanted me to add logging so they could see what was going on. The task was also designed to go beyond the handshake. It was being used to establish two-way, human trust.

After I was done, the script had been completely rewritten. Logging was the least of the issues with it. As I reported back on what I

was doing - to avoid overstepping my bounds and being written up - the trust Big Company Two had for me increased. Their encouragement and faith in my abilities also established my trust for them. I proved that, beyond our handshake, I knew what I was doing, took all necessary precautions to avoid disasters, and was making life for the other employees easier and more efficient.

Big Company Two knew I was a hacker by definition - by the very tasks they asked me to code, which required me to force interaction between applications designed not to interact - but they used humans to take the time to establish trust and determine the color of my hat, instead of simply flipping a 1 or 0 based on my job description, then forcing me into a perception that fit their handshake. Instead of a reprimand, I earned a healthy bonus in my paycheck and was encouraged to write more code.

Both companies were given the chance to use my actions to prove my motivations. Big Company One chose not to look beyond the handshake, which lead to an inevitable employment separation. Thanks to the culture and attitude of Big Company Two, we instead established two-way trust, despite the processing machine running my scripts being given a special pass by the Network Security department, since a lot of what I'd written looked like a virus. There was a lot of humanity behind that decision.

In the online era, it's the lack of perception and a real handshake to go beyond that allows shy introverts to make lasting virtual friendships - but it's the same thing that opens the door to catfishing and identity theft. On the Internet more than anywhere, trust must be earned and maintained by humans. Everyone is a stranger. You don't know who is reading your information - your tweets, your blog posts, your Facebook - nor what they're doing with it.

Everyone is a gray-hat, not just hackers. Even trusted sites can be spoofed or fall victim to a man-in-the-middle attack. This is worth remembering in a culture where most humans have ceded determining trust to machines or corporations or political parties. Human interpretation of words and actions has always been the only solid firewall against black-hats. Only what a person says and does can establish if they're black- or white-hats, from salespeople to politicians to contractors to User72 in chatroom X. It's why children are still taught not to trust strangers, and why adults have learned to neither trust nor distrust strangers.

Machines lack the depth of perception and experience that describes the human animal. It's easy to flip a 0 to a 1, but actual trust is not turned on or off. The thing we have to do, as humans interacting with other humans using machines, is add that layer of human-interactive trust to the machine's binary interaction, shading it with our perception and gut feelings and experience. It's not impossible; it just requires more work, closer attention to detail, and the realization that information on the Internet, no matter how encrypted or protected, is public, because machine trust, even two-way, so often fails.

I left Big Company One for two main reasons: 1) I figured the satellite office I worked at was about to be closed (it was, a year after I left); and 2) I didn't like the way working there made me feel, like it was us against them and everyone was doing what they could to save their necks or stab anyone ahead of them in the back. I didn't feel trusted, I didn't trust the Company, and I didn't trust my peers because that was the climate and culture the Company had created with its innate distrust of everyone.

Big Company Two knows that I could write malicious code, but they're also sure I won't. The power in trust is not that you can fool people and take advantage of them or commit crimes; the power is in not using the tools at your disposal to be a black-hat. White-hats don't use tools to snoop. They use them to find the black-hats who are snooping on others. They don't use tools to steal. They use them to make systems safer and more efficient. And while the color of a hat can be determined objectively, it is more often decided subjectively. Your actions speak louder than job titles, certificates, or credentials, but one misstep and the trust is broken.

My career has shown me that white-hats are motivated by trust and black-hats are motivated by distrust. I understand why average people - and even corporations - fear hackers, but the only way to overcome that fear is through enlightenment - through establishing human-interactive two-way trust with our actions. Humans are not binary and it hurts us to try and experience the world as if we are machines, using only a virtual handshake to establish trust.

It was too late for me with Big Company One, even if they had taken the time to see exactly what I was doing. Fear, after all, breeds distrust. It was also too late for them with me: Distrust will never breed trust, just fear. It's a vicious circle.

Jack Beltane hides in plain sight on the Internet at jackofbells.com. He writes software documentation for a paycheck, novels for his soul, and articles like this for fun.

HACKER PERSPECTIVE submissions are still closed. We expect them to open later this year so start writing now and look for an announcement in a future issue!

Software Cracking with dotPeek

by redstarx

I'm going to give an intro to peeking at other people's code.

For this example, I'll be using JetBrain's dotPeek 1.5 to get access to 5 Lives Studio's *Satellite Reign* preorder Backer Skins downloadable content (dlc).

Satellite Reign is a cyberpunk tactical strategy game that came out in August of 2015. It was kickstarted and backers got access to special content that was never released to people who bought it at release. I'm going to show you how to access that content.

The first thing you'll need is the dotPeek 1.5 decompiler software. You'll also need a copy of Satellite Reign. If you bought it on steam it will install in
`C:\Program Files (x86)\Steam\steamapps\common\SatelliteReign\`

First, you need to know a bit about what you're decompiling: Satellite Reign was created in the Unity game engine and its source code is was created using the .Net framework. Drag any of the dll files in your game installation into your dotPeek window and you can view their source code. You could have lots of fun looking at the source and figuring out the rest by yourself probably, but to save time I'll tell you which dll holds the dlc check code.

The code you are looking for is in `C:\Program Files (x86)\Steam\steamapps\`
`➥common\SatelliteReign\SatelliteReignWindows_Data\Managed\`
`➥Assembly-CSharp.dll`.

We're looking for dlc called the Backer Skins, so let's try putting skins into the search bar. Wow, so easy! We immediately find a boolean called `BackerSkinsAvailable():bool`.

A boolean is a true or false, so we know this is probably what we're looking for. If we right click on `BackerSkinAvailable()` and hit `Go To Declaration` we find this code hidden with a bunch of other gems.

```
public bool BackerSkinsAvailable()
{
  if (this.m_BackerSkin)
    return true;
  if ((UnityEngine.Object) DebugOptions.Get() != (UnityEngine.Object) null)
    return DebugOptions.Get().m_BackerOutfitsAvailable;
  return false;
}
```

Keep in mind we want `BackerSkinsAvailable` to equal true, so we need to find out what makes `m_BackerSkin` true. If you search in turn for `m_BackerSkin` you will find this code in the initial startup code:

```
if (File.Exists("BackerSkin.dat"))
  this.m_BackerSkin = true;
```

Stop and think about this for a second; if file `BackerSkin.dat` exists, then the Backer Skins are unlocked. What has to be in `BackerSkin.dat`? It doesn't matter - the code just checks to see if it's there. So just make an empty file in `C:\Program Files (x86)\Steam\steamapps`
`➥\common\SatelliteReign\` named `BackerSkin.dat` and you're good to go! You can poke around the code like this in your video games and try all types of things to get better enjoyment out of them, like reactivating cut features such as drivable cars and creating enemy agents. Have fun!

Ignore Your .env - Browsing Environment Files on GitHub

by casi

Recently, I was pushing the commit of a project to GitHub and after it was up I realized I had forgotten my .gitignore. Luckily for me it wasn't much of an issue as I was in a private repo that I'm the only user of.

This mistake made me think. If I've messed up so easily, maybe someone else has as well. I did a search in the bar for a line commonly used in .env files that I thought would bring up some interesting results.

Search: `APP_ENV=production` - 62,670 code results

This brought up a whole load of projects. I'd say the majority just have testing dev info in them with nothing sensitive, but there were a few of interest. Maybe every one in 100 would have something with sensitive data, so I would open an issue for the user just giving them a heads up (but people can't always be relying on friendly investigators).

Other times, I would find an .env existed, but was full of nonsense. That wasn't much better as it just made me suspicious. Why was it full of nonsense? Maybe if I looked in the commit history there would be something interesting.... There was.

I picked a random page, 42 sounded good. The first result had an .env with a gmail username and password!

Now theoretically, somebody may attempt to login to gmail with this info just to see if it was real. They would then be confronted with the unusual login page for gmail. This would ask them to confirm the other email address associated with the account. But it's OK because this other email is definitely not public on a GitHub profile page....

I wondered if others would also have their mail login in a commit, so I tried searching for: `MAIL_HOST=smtp.gmail.com`.

A modest 13,791 commit results. This time I tried page 26 where I found a couple more logins.

One of the .env files for a design agency blog also contained database IP, username, and password!

I tried one more search before ending my little investigation:

`DELETE ENV` - 67,226 commits

This was the most reliable for finding .env files containing sensitive data, people who have realized their mistake of uploading the .env so have deleted it in the next commit, but have not realized the commit history shows the text with the old .env in red, and the new empty .env in green. If anything, they've made it easier to see now that it is highlighted!

Here is a short list of secret things (often paired with the public keys) I found in `delete env` commits in my lunch time break. This info ranges from "oh no! I'll have to get a new key for my twitter bot" to "who made this stripe transfer?":

```
AWS3_SECRET
GITHUB_SECRET
FACEBOOK_SECRET
PUSHER_SECRET
GOOGLE_CLIENT_SECRET
PRODUCTION_DB_PASSWORD
OPENWEATHER_KEY
NEXMO_SECRET
CLOUDINARY_API_SECRET
WP_SECURE_AUTH_KEY
CONSTANT_CONTACT_API_SECRET
CHIKKA_CLIENT_SECRET
LINKEDIN_CLIENT_SECRET
TWITTER_ACCESS_SECRET
TWITTER_CONSUMER_SECRET
NEO4JPASS
BRAINTREE_KEY_PRIVATE
MAILGUN_PASSWORD
PHONE_NUMBER
DROPBOX_APP_SECRET
STRIPE_SECRET
```

You could also try other commit searches, such as: delete `application.properties`, or `delete keys.py`.

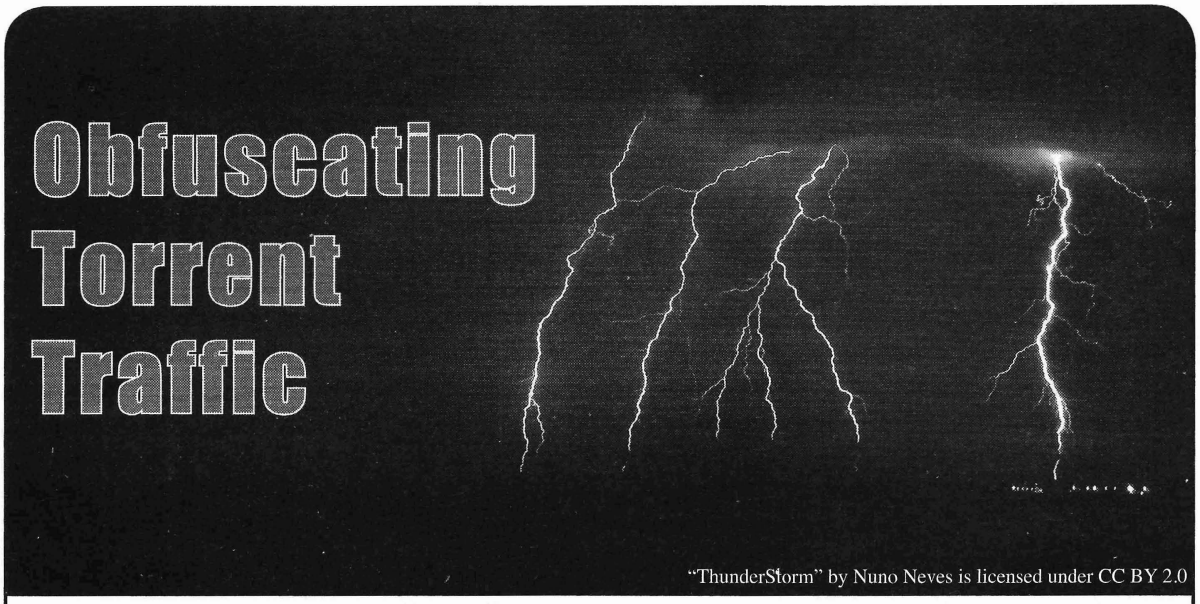
I'm writing this with the hope that people will double check their .gitignore to include environment files and key files. My searches have found that generally it is beginners and people learning to code who have decided to git without fully understanding the record they are leaving. If you introduce a new friend to git, make sure you tell them about gitignore. I also found a few repositories linked to web apps and sites trying to sell a service. How can we trust our info with you as a user if you aren't even looking after your own?!

If you do happen to commit with sensitive data and are unsure what to do, GitHub has a whole section on how to `git filter-branch` or `bfg --delete-files` in their docs. You could even just delete the copy and upload again.

If someone is looking for a way to use this, how about some kind of helpful bot that opens issues on repositories with sensitive data?

Stay safe.

Obfuscating Torrent Traffic



by Filip Kälebo
(aka flipchan)

In Sweden we have a company called Spridningskollen, which basically represents a lot of media companies. They have what I understand as some kind of mass-torrent-scanner, which is close sourced. Anyhow, these guys are real assholes. They collect Torrent swarm data and then send out threats through letters, demanding 2000 kr (that's around 234 U.S. dollars) for what they see as "stolen art." So if they see a Swedish IP downloading a torrent with any file that the companies they represent have created or have copyrighted, they will contact the ISP for that IP and get the address of the person who is torrenting down the file and send that person a letter demanding 2000 Swedish crowns. If the person doesn't pay, Spridningskollen threatens to report them and bring them to court. This is basically DMCA bad guys blackmailing regular people into giving them money to avoid going to court and opening up a legal case against that person. Anyhow, I have found a way around this using my latest project called LayerProx. Link: `github.com/flipchan/LayerProx`

So the problem is kinda that we need to secure the torrent traffic. I think that they are connecting to torrent "swarms" and just collecting IPs, but if that were to end up in court, they would need proof from the ISP that the person had been sending BitTorrent packets at that time to prove the legal case.

The way I solved this is that I wrote a socks5 support module to LayerProx that supports UDP so I can proxy BitTorrent traffic. I then bought a VPS and put up that as a Tor relay. I have removed client IP logging from the LayerProx server so that you can't really tell if there is someone just using Tor that sent packets from the server or if someone is downloading a torrent. So if Spridningskollen were to see the IP of my Tor relay, they couldn't trace it back to the client. They could, of course, trace it back to me because I have my nick on the server (`https://atlas.torproject.org/#details/AB8EE34C5CF3B6802DD1F4021FF015A463DF4572`). But this would probably not be enough to bring a case against someone in court because there is no proof that only that person was using it due to the no IP logging part.

The packets going from the LayerProx client to the LayerProx server are being obfuscated to look like regular http packets. For example, I have implemented eBay format so that it will appear as if someone is just using eBay to look at products and so on. So the packets are encrypted and then obfuscated to look like regular http browsing data. The data looks completely innocent, like a person is simply using social media and so on.

Why obfuscate/encrypt torrent traffic? If this gets big, there is a chance that the ISP will block or at least record all BitTorrent traffic. And torrents are used by a lot of good company to distribute news and media of all kinds. So the worst case scenario is that the ISPs block *all* torrent traffic. So encrypt like its 1984!

Special thanks to: Kevin P Dyer, 2600 *swedish, and the global infosec hacking community.*

Successful Network Attacks - Phase Two Network Scanning

by Daelphinux

Every successful network attack will eventually become an active event. When this happens, it means that the attacker has now committed to the attack and will do what they can to see it through to completion. This is also the first step where there are definitive ways to detect what the attacker is doing that will alert you to an impending attack.

Phase Two is the first phase that would fall under the popular assumption of what people think of as "hacking." In this phase an attacker will use a number of tools and their know-how to probe a network for any vulnerabilities, such as backdoors, known exploits, unused protocols, or weak protocols. Building on network information retrieved from the last phase, the attacker will use tools such as nmap, nessus, metasploit, the Zed Attack Proxy (ZAP), Xenotix, or Grabber to find exploits in websites, network equipment, end user devices, servers, or any other device the attacker can make a connection with (even printers).

During this process the attacker will certainly gather more useful data. In this phase, even if relatively unsuccessful, the attacker will gain a significant amount of information about your network and the kinds of devices that exist on it. Everything from IP maps, a good estimation of any subnets, network speeds, resilience, open ports on clients, appliances, and servers to any vulnerabilities in web applications. This phase will let the attacker finish determining the most viable attack vector for the real "meat" of the attack. This is the last chance for a defense to stop an attacker in their tracks and prevent the attack from succeeding.

Detecting a scan can be relatively easy. Network slowdowns will begin showing up. Once that happens, network administrators can look into access logs and will likely notice if a single IP address or small IP range is attempting to access multiple resources on multiple ports. Once this occurs, action must be taken to prevent the attacker from gathering any significant information. In more complex cases the attacker will use a botnet, or a host of zombie computers that are being controlled by malware, to perform the scan. In any event, the network administrators should be able to determine when systems are being accessed in an irregular way, but it will not be as obvious and, by the time it is realized, it may be too late to prevent the scan from being successful.

Preventing the scanning portion of an attack can be managed by ensuring that an attacker cannot gather any useful information about the attacked network. This can be achieved in a number of ways; namely the use of Network Address Translation (NAT), firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), patching, and proper administration. Each of these tools and systems has their specific use and merit; together they form a very powerful defense against this phase and subsequent phases. Each of these will be discussed at a high level as complete explanations are outside the scope of this series of articles. More information is available, at length, online and in other publications.

The first thing that an entity can do to avoid being attacked is implement a NAT solution. NAT solutions involve setting the network of an entity up in such away that all traffic entering the network is directed at a single IP address. This IP address usually points to an edge router that, with the help of other networking equipment and servers, will keep track of internal device IPs. This edge router will then be able to properly direct incoming traffic to the appropriate recipient. NATing a network makes it harder for an attacker to gain information about internal IP structures, thus making it harder for the attacker to navigate should the attack move to the next phase.

The next solutions are closely tied together. These involve setting up various firewalls with an IDS or an IPS (sometimes

both). Usually an entity, especially one with an externally facing website, will set up (at least) a pair of firewalls. One, the external firewall, forms the first line of defense and contains rules that allow incoming traffic to Internet servers, extraneousness, and other information accessible to the outside (customers, clients, visitors, etc.). Inside this area between the firewalls is the Demilitarized Zone or DMZ. The DMZ forms a layer of protection in itself by hosting servers that cannot be used to compromise the internal network and which house nothing particularly useful, while still posing as potential targets to less-savvy attackers. Past the DMZ sit the internal firewall and the IDS or IPS. These have significantly stricter rules controlling traffic moving in and out of the network. The firewall uses human-created rules to prevent malicious or unwanted traffic from accessing the network at all. The IDS or IPS, however, are more dynamic.

Both IDS and IPS can be used to heuristically determine malicious or abnormal traffic patterns and act upon them. They do this either by a set of human-created rules or by gathering a baseline of data when they are first connected to a network. An IDS will use these developed rules to determine if a traffic pattern is potentially malicious and then inform an administrator. This administrator will then look at the traffic and take appropriate action. This system simply detects the traffic and lets someone know. An IPS will perform the same monitoring and determinations regarding traffic, however if it determines the traffic patterns are malicious, it will take a pre-set action, usually cutting the connection or blacklisting the IP, and inform the administrator that action was taken. The IPS is far more active in the security process. While both are useful, it should be determined which is more fitting in the context of false-positives. If a false-positive is determined by an IDS, an administrator will take no action, white-list the pattern, and move on. However, the response time to potential threats is dramatically slower than an IPS. The IPS, in the event of a false-positive (although with faster response time), can cause lost time if it takes action against acceptable traffic. Both the pros and cons should be weighed when deciding which system to use.

Patching and proper administration also go hand-in-hand (as one *should* inform the other). However, if it is not feasible for a business to have on-staff administrators for their system and use off-boarded pay-by-hour support, at a bare minimum it should be the responsibility of a staff member to ensure network connected systems are properly updated and patched. This will ensure that known patched exploits can no longer be used as attack vectors against an entity. However, ideally there will be an administrator on staff who will ensure said patching. Additionally, the administrator should take various precautions in ensuring the systems are secure. Servers, for instance, should be used only for as few purposes as possible to perform their jobs. This way, each server will have as few ports open as possible. Further, access to systems should be properly managed to ensure that only those who need access have access to a given system. Resource accounts and shared logins should be avoided unless absolutely necessary. An administrator should also ensure that machines have the proper protective software on their systems and are regularly scanned for malware. Finally, where appropriate, systems should have file auditing active such that if a breach occurs, the attacked entity will be able to determine what data was accessed and may have been compromised.

The above defenses will prove very strong and successful at fending off most casual attackers. However, no defense is perfect. In the event that these prove ineffective, the next courses of action depend largely on the acceptable level of risk for an entity and the intentions of the attacker. In the event that the attacker simply wanted a complete listing of vulnerabilities as a test of their ability or to perform a job for another attacker, there is no more to defend against; the entity has been compromised. However, usually after a scan, an attacker will formulate an attack vector and proceed to the third phase. In that instance, the best course of action would be to prepare for an intrusion and begin defenses for Phase Three. Additionally, an entity should perform scans on their own network occasionally and patch any vulnerabilities that they find. If an entity determines that a scan has taken place, that would form a suitable next level defense.

REACTIONS

Contributions

Dear *2600:*

This is a picture taken in Oakwood, Ohio in 2016. Oakwood is an older upscale area near Dayton, Ohio, and this was taken in its shopping district. The sign denotes the street block. "2600" stands out prominently, and it's beautifully landscaped to boot.

Gabrielle

We can only imagine. And the reason for that is because the picture was never attached! We hope you give this another try as it sounds like a good image. Failing that, perhaps someone else in the area could race down and take the photo as described. (It's particularly frustrating when we get so many pictures that come with absolutely no description at all and then descriptions without pictures.)

Dear *2600:*

Good day, I am a not-so-good reader of your magazine, but that is only because I live in Mexico and it is really hard for me to find it and I don't enjoy the same reading online, but every time I can find one of your issues, I surely enjoy the hell out of it.

I am a communications manager specializing in social studies and also am a big fan of science and technology. Since I've already written a bunch of times for different publications, I started wondering if it will be interesting for you to have some articles focus on the social impact of new technologies and the way programmers work and develop in Latin America. I work with an American editor so I can send you the articles in proper English.

Let me know if we can find a way to collaborate. I am open to any suggestion you may have about my approach to the subjects.

I appreciate the attention and stay at your service.

Vanessa

We most definitely would like to hear your perspective on developing technologies and the effects it has in a different culture. Having already read our magazine, you get where we're coming from and know it's about so much more than just the latest security holes. We think your words will open lots of eyes. Thanks for thinking of us.

Dear *2600:*

I used to read *2600,* as I grew up an ethical hacker turned entrepreneur. For too many years, Internet and technology corporations and government actors corrupted by haters have abused their power and enabled sabotage of my personal and professional lives. You should read about it on my blog and do a story on me because your audience would be most interested and we cannot let frauds get away with it.

Russell

If you can write a letter to us saying we should write an article about you, we think it's highly likely you can write an article about the things that make you interesting enough to write about. If you want, we can put that in writing.

Dear *2600:*

I'm not sure this is the correct place to do so, but please find attached a photo I would like to submit for the cover of *2600*.

Jason

Thanks, but we already know that the Watergate Hotel in Washington DC has 2600 as their address and that in itself just isn't enough for a front cover. It might have worked for a back cover but we've already pointed attention at this. Plus, people aren't really in the mood to be reminded of Watergate these days. Thanks for thinking of us and please send us any other ideas.

Distribution

Dear *2600:*

I am interested in your magazine and wanted to know if there is a newsstand location in Los Angeles that carries the current issue.

John

If you can find a newsstand that carries lots of magazines, we should be in there. If not, ask them who their distributor is and we can talk to them about getting carried. We're still trying to get lists of sales points for our readers and will stick that on our website when we get it from our distributors. We do get carried in all Barnes and Nobles and if there are any other bookstore chains left, there's a good chance you'll find us in those too.

Meetings

Dear *2600:*

I with peerlyst.com, a community serving over 100K security professionals.

We heard about your meetups and wanted to help you make more out of them.

Early this year we have announced a formal partnership with Bsides Las Vegas, where we became Bsides' formal community platform. We wanted to explore the option to execute a similar initiative with you, to make more out of your events.

Here is what we did at Bsides:

L

Let us stop you right there. We really wish people would look into our meetings just a little bit before sending us these corporate pitches. As described in our guidelines, our meetings are informal and open to everyone. We don't need or want partnerships, meetings aren't limited to security professionals, and we're quite happy with how they work as is. Please stop by one of them and see for yourself. Share info, listen to stories, make new friends, but please don't try to sell us anything.

Dear *2600:*

I wanted to give you an update on the Vancouver *2600* scene.

Since Defcon 2016, a small group of us have committed to showing up at every *2600* meeting possible. We have been going strong since August. Attendance is picking up. We now have around five to ten people showing up. Pretty good.

I spoke to a regular attendee and he's very happy that folks are showing up again. Seems like the meeting was dead for a bit as it happens.

Anyways, we'll keep the light shining and a welcoming seat open each first Friday of the month for our fellow enthusiasts.

notaspy

Thanks for the update and for keeping the spirit. Meetings reflect the enthusiasm level of whoever happens to be around at the time. All too often, people don't think they have the power themselves to really make a difference, both at meetings and throughout life. We want to make sure that as many of us as possible get to realize how untrue that is. If your local meeting isn't as good as you think it could be, simply making an effort to find other like-minded people often pays off. It doesn't happen overnight and the first meetings are usually the hardest. But once it becomes routine and not dependent on any one person, they begin to take on a life of their own. Then they're impossible to stop.

Dear *2600:*

We're starting a *2600* group in Petaluma, California. We have had one meeting last month and having another this month on the first Friday at 6 pm. We meet at the Starbucks downtown by the fountain. We have a great group of security researchers and we are still growing. I hope you can post us in the magazine so we can grow even more. Thank you and speak to you soon with an update.

MG

Good luck with your new meeting. If you continue to give us updates, you will be listed in the magazine and on the website, which should bring in a bunch of new people. It's great to see this tradition continue and get reborn in new places on this, the 30th anniversary of our very first meeting.

Dear *2600:*

Edinburgh (Scotland) had its second *2600* meeting yesterday, the 3rd of February 2017.

We had much more activity than at the first meeting. Around 15 folks showed up and all got to know each other. There were a variety of backgrounds which was great to witness.

We even got to do a bit of urban exploration, which if you know Rose Street on a Friday night in Edinburgh can become quite an adventure!

The plan going forward is to keep doing these meetings. Eventually we might attempt to have short talks to try and spice things up a bit.

stmerry

This is so great to hear, considering there weren't any meetings at all in Scotland only a few years ago and now there are two. It sounds like you've all got precisely the right spirit and will continue to draw natives and visitors alike to your venue for the foreseeable future. This isn't the only letter we received concerning this meeting. Another reader wrote in to tell us the URL for the meeting's website. It's 2600edinburgh.org.

Dear *2600:*

First of all, please receive my congratulations for the good work you do. I have to admit I just found out about you a year ago, but it is good to have found old-school guys around. When I was 16, we used to read magazines like the one written by the "RareGaZz" team, and browse FTP server repositories as one of the ways to find interesting information. Now with everything interconnected, everything is accessible almost instantaneously, and the possibilities to explore have also grown a lot.

Quick question! I posted you some time ago in order to ask you for some support as I was planning to start a *2600* meeting in Spain. I haven't received any reply from your side. Can some of you guys give me some advice about the next steps to register in your meeting list?

Many thanks in advance, and keep up the good work.

Echo

We don't know where you might have tried to communicate with us in the past, but it's likely we wouldn't have replied from many of them. The letters are where we focus our main reply attention, so right here is the best place to look. There are people who expect quick answers to every inquiry and we just don't have the time to make that happen. But for meetings in particular, we have an auto-responder set up that's designed to answer most any question that comes up with regards to starting a new meeting. So if you email meetings@2600.com, you'll get a bunch of info back right away that should be helpful. Please don't ar-

gue with our auto-responder because it will give you the silent treatment after your second email. (You would be surprised how many people think they're talking to a rapidly-typing human who managed to crank out a multi-page reply in ten seconds just for them. And of course, they expect another instant reply right after that and then get furious when it doesn't arrive.) We hope you're successful in bringing meetings back to Spain. Please keep us updated.

Dear *2600:*

I'm from Goa and I'm interested in attending meetings. But there aren't any meetings held in India. What can I do?

Dinesh

Thirty years ago a bunch of us in New York were also interested in attending meetings but there weren't any. So what we did was start them! You can too. It doesn't matter where you are (unless you're in one of those parts of the world where meeting publicly and/or anything hacker-related is considered a crime); you have the power to get them going on your own. It may seem like a daunting task and, sure, it would be easier if someone else did this. But we all know that's not how things actually get done. More times than not, we have to do them ourselves.

You'll find all of the guidelines you need to have meetings at our website (www.2600.com/meetings) or you can have them sent to you by emailing meetings@2600.com. We really hope to be hearing about meetings all throughout India in the future.

And incidentally - and as testament to the surprising power we all have to change things - your letter was actually sent to us as a Direct Message on Twitter. That made us realize that this is another way people can communicate with us here at the letters department. Our Twitter ID is @2600 and anyone with a Twitter ID can send us a message. We honestly hadn't considered receiving letters in this way, but your message inspired us to give it a try. Now that you've accomplished that, starting a meeting doesn't seem so hard, does it?

Storm Warning

Dear *2600:*

Honestly, in light of the new powers the NSA has and everything else going on in this country I don't want to be associated with you anymore. Thanks for the issues I did receive and if you could delete my info from your databases, that would be great.

Name Deleted

You're not the only person who has reacted this way since November. That is something we find very disturbing and it led us to issue the following statement to our readers at the end of the year:

"A number of people in our community feel that hackers in particular will be under increased scrutiny and will be facing significant threats under a Trump administration. We've received requests from both readers and writers to erase all evidence of their existence in our correspondence and to cancel their subscriptions and remove their names from our database. On more than one occasion, all hacker-related clothing was also thrown in the trash.

"It's this reaction that we find more disturbing than any of the many potential threats we're facing. Why? Because bad things happen when people let them. As long as we stand united and are willing to fight back against anything that would threaten us as individuals or as a community, we have what it takes to prevent such threats from taking hold. If we yield, it's handing out a blank check.

"Yes, there is much to be concerned about and even to fear. Hackers, as always, seem to be right in the middle of the controversial news stories bombarding us every day. But we need to embrace this, not push it away. We have always protected the confidentiality of both our subscribers and those sources who contribute material to our publication. We will never stop doing this.

"There is great strength in numbers and in intelligence. We need both in order to survive what may be hugely challenging times. We cannot let the specter of oppression slow us down because if such a scenario were to come true, that is when we would be needed the most. We should have more articles than ever, edgy and controversial material that we embrace, and a ton of people who aren't afraid to read and collect what we're putting out. After all, it's in the darkest hours when a bright light makes the most difference."

Since then our resolve has only strengthened and so has that of people all over the country. We believe that what we do and what we believe in is stronger than anything that seeks to control, diminish, or destroy, particularly using fear and ignorance as its allies. But we can only speak for ourselves; we pass no judgment on anyone who feels the potential sacrifices and risks are too much for them to bear. We believe our community is strong and will ultimately survive and flourish. In fact, this may be exactly what was needed to wake people up who took a lot of things for granted before.

Dear *2600:*

So with our recent election of the *wrong* person *again* (two prior Bushes!), I won't go into the details of how those elections were stolen. But since you have posted about these things in the past to one degree or another, I thought I would pose these thoughts to you.

Reportedly, Wikileaks was somehow able to

get information on Hillary Clinton and the email server debacle for which she was acquitted not once, but twice! What I propose is that through the appropriate channels (Wikileaks, etc.) that our blustering, boastful, blithering idiot President be investigated to the same degree that Hillary was!

Things are only going to get worse as the country gets Trumped to death; the rich (people, corporations) are going to get *so much richer* under Pet-rump and the rest of us will be picking up the tab for the giveaways!

I can submit follow-up documentation proving my point and other supporting points, but must get to work.

I have enjoyed the publication for years. Keep up the fight!

Pissed off in Long Beach, California

We can't say what did or didn't happen because we don't have the information. Whoever does have that information (or the ability to get it) has, in our opinion, a moral obligation to share it with the world so we can see for ourselves what did or didn't happen - or just how clean or dirty certain hands are. There certainly seems to have been some strong bias regarding the leaks that were revealed. It's hard to imagine that one side had bad security and one side had good security and that's where the story ended. We aren't fans of any particular candidate or political party. But we do know when something smells rotten. We've been heartened by the reaction so far and there is no corruption on earth that can stand for long against that level of pressure.

A Look Back

Dear *2600:*

Going through some boxes in the attic today and I came across Volume Fourteen, Number Three.

Perhaps you could reprint the epigraph about confidential information being transmitted over pagers and the article titled "Hacking the Vote."

They're both so quaint, and remind me of a much more innocent time.

Selah,
Dr. Dave

It's interesting that you came upon that particular issue, as we've just released it digitally as part of our Hacker Digest *project, so quite a few people are probably seeing it for the very first time. As you've already discovered, this stuff never gets old. In fact, the leaked White House pager traffic we released back then (1997) is being put up on our website after apparently disappearing from nearly everywhere else on the net. One thing this project has taught us is that, despite common belief, things can disappear completely from the Internet if you don't look after them. That's why we're working so diligently to preserve our history.*

Dear *2600:*

It's amazing to see what has been lost over the last few decades, and how things are progressing. Gone are the days of exploration, replaced with convenience and spoon-fed learning.

During the eighties, if you wanted to learn about UNIX, VMS, or any other operating system and equipment, you would have had to obtain access to these systems, which in turn taught many how to use them. It made you work for it, and it pushed you to learn. There was a 2003 movie, *In the Realm of the Hackers* (the story of Electron, the hacker from Melbourne), in which at the end he mentioned "Today there are automated tools to do what took us weeks or months to learn how to do." And this couldn't be more true.

The thrill of sharing information from a BBS is gone. No longer do you need to telnet into a UNIX machine to learn. A home PC can now run ten virtual operating systems, and emulation and the cloud are the new way. Even the sounds of the old phone systems are long gone, and replaced with the silence of VoIP connections.

We are every day being moved further into a world of more convenient learning, rather than being pushed to work harder to seek the answers.

The term hacker, when said in the seventies and eighties, would have meant someone gaining access to a system, seeking answers, and learning things we weren't intended to know but curious to find out. But in today's world, the hacker is made out to be the evil ransomware sitting in a dark corner of the world. It's unfortunate that times have changed, but at least for us true hackers, we will always know the true meaning of exploration and seeking the harder path for answers.

Darkmatter

There is a good deal of truth in much of what you say, but we can't share in all of the pessimism. As long as there are new things to experiment with and develop, the spirit of hacking cannot disappear. What changes are the specific tools. Clearly, things can't remain the same forever and technology is always improving, getting faster, and standardizing. Who knows what the next step will be? But the most exciting ones will be those that encapsulate all of the values you defined above. Look back into history a bit and you will see that with every change that takes place through our technological or social evolution (wire recordings to vinyl to CD to digital downloads - Morse code to radio to television to YouTube channels - cordboard to step to crossbar to electronic to digital to VoIP, etc.), there will always be people who look sentimentally back at the way it used to be as well as those who only look forward and have little interest in the old ways. We benefit when these people talk to each other and share the values and magic of both the past and the future. We can nev-

er really see what's coming, but we can guarantee that we will one day look longingly back at these as the good old days.

One other thing: hackers of the seventies and eighties were also seen as evil and misunderstood more often than not. There just weren't so damn many of them back then.

Feedback

Dear *2600:*

In *2600's* response to david0509's letter on Lightweight Portable Security (LPS) in the Autumn 2016 edition, there is a reference to some errors in the browser. The errors you are seeing is because the DoD has their own root certificate that is not trusted by default.

If you check the root certificate on that site (and probably for any public facing HTTPS DoD site), the root cert is "DoD Root CA 3", which is not in your certificate store.

Once you install the root certificate, the certificate error will disappear as the remote servers are now trusted. The DoD even has an installer for them! You can find it at http://iase.disa.mil/pki-pke/Pages/tools.aspx under the "Trust Store" tab. If you feel comfortable installing a root certificate from an HTTP page that has no checksum value for the file, that is. You could also use your systems certificate manager or the classic: ignore the security warnings.

Keep up the good work and look forward to playing with LPS.

kes

Dear *2600:*

I just received issue 33:4 and read with some astonishment the paranoid ramblings in the article "Spying Across Borders in the Age of Email." In the article, a technology researcher (?) and a Brazilian colonel with 25 years' military experience (?!) freak out about the UK's Ministry of Defence (MoD) apparently hacking into their Outlook email.

The writers place the incident in the context of international espionage, becoming outraged when neither the MoD nor Microsoft want to "admit" that they have been the victims of international cyber-espionage.

So far, so exciting. But it's time for a reality check.

A cursory Google search - something like "uk ministry of defence ip address" - brings up plenty of information about what's really going on here. Surprise, surprise - the MoD aren't hacking into people's Outlook email at will with the collusion of Microsoft. The IPv4 range 25.x.x.x was originally allocated to the MoD, back in the early days of the net. But things don't stay the same forever.

Explanation One is that some of the IP range has been sold off, and nobody bothered to update the entries at RIPE. That could be true.

Explanation Two is that some services, such as T-Mobile and Hamachi (LogMeIn's VPN service), are being a bit naughty. When they run out of allocated IP addresses, they switch to ranges allocated to big government agencies that are unlikely to cause a problem. In this case, some service was (ab)using the 25.x.x.x range, on the basis that there's unlikely to be any crossover between the users of a commercial VPN service and the UK Ministry of Defence.

Those explanations could be wrong. But Occam's razor suggests that either one is more likely than the convoluted story of a remote foreign power not only breaking into someone's Outlook, but leaving a very obvious trail behind them. And all it took was 30 seconds on Google. Maybe I should become a technology researcher... then again, maybe I'm not paranoid enough.

YTT

Dear *2600:*

The code is missing from the Autumn 2016 article "Spyware Techniques by Chuck Easttom. I had purchased the Kindle version of the magazine. Additionally, when I checked on your site (www.2600.com/code, it was missing on the site too.

It would be great if you could share this particular article's code.

Sudarshan

The code appeared in our test Kindle version. We'd like to know if anyone else experienced this issue with their Kindle copy. By the time you read this, we hopefully will have replenished our code section, which once again fell into disrepair.

Dear *2600:*

Just thought you'd like to see how nicely the magazine is displayed at Micro Center in Houston. I had no trouble finding a copy.

brucerobin

OK, that's a bit insane. Did they actually give us all that space or was it an overly enthusiastic and super supportive reader? If we had this kind of exposure everywhere, the world would be a different place.

Dear *2600:*

I just read the Winter 2016-2017 issue and took note of El Magistral's comments about the

"alarming decline in quality of the articles." There's a very easy way to solve this. It benefits us all. And best of all, it's completely free.

What anyone can do is email an article to articles@2600.com and, if accepted, it will run in this fine magazine, raising the quality of the articles.

While we're talking about quality, "Telecom Informer" continues to be my favorite. Every quarter, I first read the opening section and then immediately jump down to see what The Prophet has gifted us with this time.

John

Thanks for the kind words. And what you say is true: the higher the quality of articles we get, the more high quality articles get printed. But we don't want to discourage people from bitching and moaning even if they don't have anything better to contribute. That, too, carries its own special magic.

Dear *2600:*

I am wondering what is happening with your Amazon Kindle edition? I tried to buy your latest individual issue on Amazon (33:4) and it said there was no issue available for the Kindle app iPhone version? Same thing happened when I tried to subscribe. This is their message: "This publication is not available for some devices. The publisher may have opted out of making it available on certain devices, or the reading experience may not yet be optimized for this publication on those devices."

I was able to buy the previous three issues and read them on the Kindle app for iPhone OK. Except the last one (Autumn 2016) was odd. It had no pictures except the front cover. No payphones, no article illustrations. Another odd thing was it had a word count at the top of each article. Maybe I did not get the final file? Should I download it again?

I really like your PDF versions that your annual digests came in. I like how they have page numbers and look like the print version. Could you do the individual issues that way so I can buy them directly from your store instead of buying them through Amazon?

Inquiring Mind

Sometimes Amazon has glitches that affect certain devices. It's almost always cleared up within 24 hours of a new release. All issues should definitely have pictures, so please grab that one again and it should be fine. Whenever you encounter a message from Kindle saying that we (the publisher) changed something or didn't do something, please don't believe it as nearly every problem like this that's come up over the years hasn't been on our end and we lack the access required to be able to do that sort of thing in the first place. Despite the occasional frustration, we still think the Kindle edition works quite well and it seems to be extremely popular. We're considering all kinds of other methods of distribution. Your suggestion may be one we try out in the future.

Dear *2600:*

Hey gang, I'm sending this email because it seems that Amazon/Kindle has crapped on *2600,* unless you are the ones who did it.

"Kris, we did not find a Kindle device or reading app registered to your Amazon account for which this content is available."

Funny thing is, just the latest issue, which I had already gotten, downloads and reads just fine. I can subscribe through other means, but most of my magazines are through Kindle, but sadly, at this point, you're not the only magazine this has happened to me.

If needed, I can provide screencaps of the relevant devices, but as you're probably aware, it's all Kindle devices and nothing else.

Thanks!

Kris

The fact that we're not the only magazine where this has happened again makes it clear that this was a Kindle problem which we trust was resolved. For future reference, contacting their customer support is almost always the fastest way to have these issues cleared up. We have no access to the Kindle subscriber list, we're not making any changes to access levels, and every one of our issues is thoroughly proofed and doublechecked before being released to them. We do want to hear about any problems people are experiencing, however, so we can add our voices to the chorus. Hopefully these are just growing pains.

Dear *2600:*

Thanks for publishing my article (Free Windows) in 33:2. I noticed a question about the article from db in 33:4. Here is an answer for db:

Thanks for your interest in Free Windows! Free file hosting sites are ephemeral, and their links can be very short-lived! So here are more mirrors for the MS Toolkit:

tinyurl.com/zx7n2fm
tinyurl.com/toolkit-2-6-5
tinyurl.com/2-6-5-ms-toolkit
www.embedupload.com/?d=8JBHFEHXAN

(The first link requires sign-up with 4shared, but this is free.)

As of January 27, 2017, most of the links in the References section of the article are still working. The second link is gone, but you can still work with the instructions in the article to create working iso files using the MCT. The fourth link in the References, for the clean Windows Toolkit app, seems to not be working, but hopefully the above new links will help. The Toolkit contains the AutoKMS. Note that it should be possible to use Au-

toKMS separately from the Toolkit, but the Toolkit is preferred since it provides an easy way to install, test, and maintain (manage) activation status.

fooCount1

Dear *2600:*

I always enjoy the Telecom Informer articles. His latest (33:4) is great, but a little bit incomplete. Rogers and AT&T did not go directly from AMPS analog cellular to GSM, but spent quite a few years using IS-136 TDMA. TDMA, as it was known (GSM is also TDMA, but was never referred to as such) had some technical advantages over GSM (it used less bandwidth, for example), and achieved quite a bit of penetration in Latin America and Asia as well as North America. But it was not compatible with GSM. The network was based on the same protocol (ANSI-41) used by AMPS and CDMA2000. Rogers and AT&T were well on the way to phasing AMPS out well before they switched to GSM, as TDMA-only phones were much smaller and had significantly better battery life. They jumped to GSM because there were more GSM phones available around 2000, and they were cheaper. And once they switched to GSM, they stuck a knife in TDMA, withdrawing support for the North American Cellular Network (NACN) that provided TDMA roaming, forcing carriers all around the world to plan their own migration (mostly also to GSM).

Additionally, while it is true that the first iPhones were GSM-only, for a long time it has been possible to get iPhones that work in both GSM (including LTE) and CDMA2000 modes, so there is really no disadvantage any more. In fact, given the slow rollout of VoLTE (Voice over LTE instead of fallback to CDMA2000), CDMA2000 will be supporting phone calls for a long time, while getting no praise or glory. There is a rumor that Verizon was offered the iPhone first, but they thought Apple was too greedy. AT&T took the attitude that if the entire executive suite had to commit self-defenestration or, worse, pay their fair share of taxes, they would have agreed, in order to get the first Apple phone. If Verizon had had a better crystal ball, things would have turned out a lot differently, although in the end, GSM would have been added in once the exclusive agreement with Verizon expired.

D1vr0c

The Prophet responds: "Great letter, and thanks for writing! For sure, the short-lived TDMA standard is a correct historical footnote. Additionally, Telus operated an iDEN service for many years using the brand name 'Mike.'"

Asking

Dear *2600:*

Good afternoon,

My name is Stas. I am 15 years old. I have a little different hobby: I collect badges (pins) and stickers with symbols, seals (mascots) of companies, and arms of cities. Could you please send me your badge? Thanks in advance and sorry for your trouble.

Stas

Belogorsk, Russia

Sorry to burst your bubble, kid, but you're really barking up the wrong tree here. (At first we thought this was some especially weird kind of spam, but it appears to be on the level. This guy really collects badges, pins, buttons, or whatever you want to call them.) Decades ago, we had 2600 *buttons but nobody has seen one of those in ages. We have a corporate seal someplace, but it would probably take us a few months to track it down and it's probably something we're not supposed to be handing out like candy. And we don't even know what "arms of cities" look like, but we're pretty sure that's not a thing in these parts. But otherwise, we're in full support of what you're doing and hope we've helped somehow.*

Dear *2600:*

I am UI/UX, web, and mobile graphics designer and developer looking for work. Examples of my work are attached. There you can find any kind of design work you need. My portfolio is the largest web design portfolio on the Internet. It contains 180 designs sorted under 35 categories.

Marko

Largest web design portfolio on the Internet? That's quite a claim. We were quite impressed with the massively huge attachment you stuck in that email, but not enough to want to go any further than this reply.

Dear *2600:*

With due respect I m using airtel operator . there is very bad networks voice call and internet.please solve my problems as soon possible. Thanking you.

Shazia

Every now and then we get one of these emails where we wonder if we've crossed into some sort of TV plot where we only have a few minutes to solve some high energy crisis and save the world but we didn't check the email until weeks later and apparently lost our chance. But on further investigation, Airtel isn't a phone service inside an airplane, but rather a mobile operator in India. So the problem cited is probably one of months or years, not seconds. So we feel better about that, but we still may never know what this was all about. Unless this guy is just asking for the name of a better cell phone company in India, to which we'd suggest Vodaphone India, Idea Cellular, Jio, or RCom. Of course, had we visited India instead of Wikipedia, we would probably have come up with a better answer.

Dear *2600:*

I heard that the president of the USA can text everyone at once in the whole USA with a special message.

I, for one, refuse to accept anything from Trump anytime.

Is there a way to block such a system? Or is there an app that can block that for me?

Moshean

It's called a Wireless Emergency Alert and there are several kinds. You may get a WEA message if there is severe weather in your area, an evacuation order, or an Amber Alert for a missing child. Those alerts can be turned off in the Settings section of your phone. Then there are the Presidential alerts, which cannot be turned off. You can't even turn down the volume without turning your phone off completely. You can blame Congress for that. When they passed the "WARN Act" in 2006, they explicitly allowed participating carriers to offer subscribers the capability to block all WEAs except those issued by the President. But you may be able to find a way out before Trump figures out how to abuse it. While consumers aren't able to opt out, it's voluntary for carriers to opt in. So you might be able to track down some cell phone company that doesn't support WEA. Perhaps that could even become a selling point for them. Of course, in so doing, you also could wind up being the last person to find out a tornado is heading your way. That's the disadvantage with these systems being overused or abused; people will wind up ignoring them when they are really needed.

Dear *2600:*

I have ordered several audio DVDs of the various previous HOPE conferences. I would like to distribute them over the Internet. What is your policy regarding the sharing of these audio files over the net? I will follow your direction.

WarmFuzzy

It's really quite simple. We want them shared and copied as much as possible. If you put them online, just give a link back to us (the 2600 site, our store, or the HOPE site). This is true for the contents of our DVDs or flash drives as well.

Dear *2600:*

I am looking into several business endeavors, some of which will be relevant to your magazine. Therefore, I'm interested in buying advertising space. Could you possibly email me with your current advertising rates for various ads (full page, half page, etc.) including the number of and type of readers you have (e.g. hobbies, lifestyle)? I look forward to hearing from you.

Jeff

If you had any idea what our magazine was about, you wouldn't be looking forward to our response. Do you see any advertisements in these pages? Other than the free classifieds we offer to our subscribers and the house ads to publicize what we're up to, we simply don't go down that avenue. We're 100 percent reader supported and that's how we want to stay. We have no interest in prying into our readers' hobbies and lifestyles, nor of taking away valuable pages to advertise already over-publicized products. So this is why you will not be receiving a list of our advertising rates. If you become a subscriber, you can have a short classified ad for free. We hope that suffices and that our message has been received. Until the next time someone asks us this, which has probably already happened.

Leaks

Dear *2600:*

With all the bogus accusations about "Russian hackers" flying about, certain questions keep coming up which only the hacker community would appreciate.

If "the Russians" really did "hack," then they would *never* have left any trace behind.

It has been said that a DNC insider who favored Bernie Sanders and objected to what the HRC people did to him "leaked" the information.

WikiLeaks has established itself as "a media outlet" with unimpeachable accuracy.

All WikiLeaks will say is that they did not get *any* of the emails from the Russians!

Just like any "American media outlet," WikiLeaks must be given the *right* to protect their sources. Only the accuracy may be brought into question and that can be assumed to be unimpeachable!

Clearly, all of the noise is about a vain attempt to have the "leaker" exposed, "plug the leak," and punish that individual(s) so that even more damaging information might not be leaked!

Since I used to work on the computers used by the Department of Transportation in more than one state, I know this simple fact.

If the "Russians" really wanted to cause any kind of chaos, all they would have to do is inundate those systems with data which would attach and cross reference aliases and addresses to as many people as possible. Especially judges and politicians - the police are just pawns.

I found this out by accident when I tried to get my "home address" information corrected since I am technically "homeless." It is impossible for any government computer to make any kind of correction. The government simply sends papers to whatever address is last on the list without verification of any kind. All challenges to such information are summarily rejected. Very interesting. Those computers keep everything, although I am curious as to just what the "limit" to each data field might be (256, 512, 1024)?

Why protect something which can be used to do you harm?

Homeless Man

Where do we begin? Well, we have a limited amount of space, so let's stick to the simple points. While it's our default state to question and doubt anything we're told, that rule also applies to anyone who states with certainty that a particular fact is "bogus" without any actual evidence. In this case, defining terms becomes hugely important. Very few people believe (or are saying) that the election was literally hacked on Election Day by Russian hackers. In fact, the only people who seem to be quoting that are those who want to demonstrate what a ridiculous notion that is. In actuality, the involvement of outsiders in the electoral process would be much more subtle and prolonged. It would most certainly involve various infiltrations, disinformation campaigns, and leaks. Done in a methodical manner, such actions could most definitely have an effect on the outcome of an election. In fact, our own country has a long history of doing precisely this, as do others, including Russia. So in theory, at least, such a hack is possible. Sticking "it has been said" in front of a specific theory is a familiar tactic, but adds absolutely nothing of value to a conversation. We found it odd that WikiLeaks would go to the trouble of saying where these particular leaks didn't come from since anonymity is such a vital part of the leaking process. From their own site: "We keep no records as to where you uploaded from, your time zone, browser or even as to when your submission was made." How then, do they know that the leaks didn't come from Russia? And, if this is true, doesn't revealing such information help to narrow down the actual source? These questions sort of chip away at that whole "unimpeachable" thing you were mentioning.

Obviously, victims of a leak will want to find out where it came from. That shouldn't be surprising to any of us. But when the leaks only seem to be affecting one side of a contest, then you have to start considering if there may be an agenda at play. And if your attempts to get to the truth are resisted or blocked, then you really need to start rethinking the possibilities.

Dear *2600:*

I know of rats in your company now Jimmy [last name redacted], Ken [last name redacted], Terren [last name redacted], Charlotte [last name redacted], and security owners UK/Ireland, Faye [last name redacted] (ex-New Yorker but not American) and many others is all holding was cards for government and should warn your experts straight away cos they are terrorising me and my underwrls tens with 5o,.!... .

Be carefull bro's as we are turning anything but grey now on them but blk only.

Try outwit for your own safety as I have nothing to gain and have nothing to gain from this at all except give in as my only way out or fight back. Trck this locality's pths and no: please plus [phone number redacted] and my connecting emails.

Safe braheims,

[Everything Redacted]

We actually do get more cryptic messages than this one. Considering we never heard of any of these people supposedly in our company, they must really be doing a good job.

The Future

Dear *2600:*

I would like you to publish this letter (I'm a CIA operative):

2200 or 2600? Space Age

1. Arrests of hackers and those who authorize assassinations and transmit death threats in moments after they do so.

2. Food and shelter and income for all so that no one wants.

3. The legalization of sex work and all drugs and fights to the death.

4. One-hundred percent dependence on solar.

5. Widespread space flight for the people.

6. Free higher education for all.

CIA referred me to this site to learn about extraterrestrials. I hope it helps you all with your struggles: www.bibliotecapleyades.net/vida_alien/esp_vida_alien_19a.htm

Robert

Wow. Just wow. At last, a list of aliens in alphabetical order. You have no idea how annoying it's been to have to wade through so many unorganized collections. So thanks for that. As for your list of whatever it is, we're happy to see that our arrest is literally at the top of it. It's a tad disturbing that we're lumped in with assassins and death threaters. Everything else sounds so good, though. Except maybe legalizing fights to the death, which seems like an awfully strange thing to campaign for.

Dear *2600:*

What will happen today? What will happen tomorrow? None of us ever consider that question thoroughly when we wake up. We usually expect the worst and hope for the best. What will happen next year, what will happen in the next four? This seems to be a common pattern in my mind while, yet again, most people expect the worst and hope for the best, the worst being a madman with his hand on the biscuit and some inept gerbil sitting elsewhere with the inability to disregard an unlawful order, holding the football... expecting the worst... but no hope? That puts a smile on my heart because we don't truly believe that. When there is no hope (in our minds), some will cower, but others have no fear and realize that some-

thing has to change. During the circus tent fire, we were given the option of a compulsively lying war criminal with bad experience, or a man with no respect and no experience. Yes, you heard me correctly folks, the gun is loaded and in your hand. Now point down and choose: *left* foot or *right* foot - which foot can we empty this chamber into that would not leave us limping afterwards?

Yes, you heard correctly; but what can we possibly do?! We *have* to choose, we just have to! Yes, life is full of choices, but it's not our choice anymore. If nothing we choose will be best for the people, I believe in the people, oddly enough.

I once said if Hillary gets elected, I fear for the future of this country, and if Trump gets elected, I fear for the near future. I imagined that people would go along and take the slow route and not vote for Trump, and slowly let the country continue to rot, so slowly that it's hardly even noticeable, but *now* there's a malignancy in the system. The people are the antibodies and can *notice!* A great big smile on my heart indeed - where voting for one would be a rootkit with concise and indiscernible code, the other would be a very sloppily written Trojan that wouldn't make it past the most primitive of system defenses.

Yes, I'm happy, not because the worst fears of many came to fruition, but because now is the time to fix the system and people are aware more than ever about what they have been letting take place. This country is not living up to its full potential. I'm no super hero - hell, I'm not even better than average - but how amazing is just one antibody? Maybe beautiful in its own way that a blood protein can be created, seemingly pointless on its own, but there are people that want the antibodies cloistered, and to themselves. Together we can fight, without violence maybe or breaking the law, but coming together to face a threat. If the virus isn't noticeable, the body just does what it does. But when it gets really bad, there is a panic. But is the panic something to be concerned about? The body discharges and coughs and sneezes and the fever kicks in trying to heat up and burn out the malignancy, almost as beautiful and synchronous as the Japanese honey bees rubbing together when there is an intruder like a killer hornet in their nest - all together, at once, harmoniously never raising their temperature to the point where they themselves would be injured, but just enough to where the hornet would not last in the hive. The hornet is a scout for more dangers, but when the bees notice, they don't let that report ever leave the hive. The hornets never get the message, the hive becomes a haven, intact, a place for bees to create their honey and live a prosperous life.

Trump is a message to all voluptuaries with no experience around the world, like the reconnoitering hornet in the hive of the Japanese honey bees. All he has to do is get away with doing terrible things, and that is the new paradigm forever and ever until the end of times, but having no experience can be overwhelming, especially if the bees turn up the heat and present real problems, needs, and requests, and make it so intolerable that the hornet simply cannot stand the heat. Yes, a true test of one's character is to see if they can handle the heat and make right decisions, or if they say, "fuck it, I can't do this." But it seems as though these hornets have a highly evolved strategy. If only the antibodies were as advanced and evolved, yes?

Doesn't it feel good knowing that for once the antibodies have something they can recognize, and unite to make a difference? That's called *hope!* If our forefathers were here now, they would see what I see, what we all see now, a broken system that needs a bit of tinkering, dare I say... "hacking?" Yes, I'm ordinary. A lot of us are. But one puzzle piece may not seem like a big deal, unique, but piled on top of all the other pieces seemingly identical in its uniqueness. But something is beautiful to behold when all the pieces come together. We see the big picture. Sure, there's the obnoxious guy that wants to keep breaking up the puzzle so we can't see that big picture, but I have a feeling now that our minds have evolved with playful little jests, pranks, and even disassembling, we have learned to take apart and put together better than ever, our own personal DHT. They can pull apart, but we check the hash sum and put together three pieces. While they take those three apart, three other pieces come together. And when they take those three apart, all six already confirmed they go together, all six come back together and boy, is that frustrating for people trying to separate the puzzle.

Let's just bear in mind that one bee shaking and rubbing another bee won't do the trick; it works best when all bees are working together. We are all different like the puzzle pieces, but we shouldn't focus on the little bumps and ridges that make us different, but where we can plug ourselves in to help everyone else get the big picture. Fuck the planet, hack the system, forever and ever until the end of times.

Devlin

It's strangely comforting to be using the same tactics as bees.

Dear *2600:*

I perceive massive amounts of doublespeak about fascism, racism, net neutrality, and many other subjects. It has reached a point where I am almost ready to give up and follow the Church of the SubGenius. Am I alone?

Thank you for existing. *2600* is an island.

colForbin

You are far from alone. That realization, along

with some organization (perhaps similar to the bees referenced above) is all you need to make real progress. Reaction to adversity is key. We push harder when we fight back than we do when we're comfortable. So this is an opportunity for real progress.

And as for us being an island, thanks, but in this age of climate change, it might not be the best thing.

The Marketplace

Dear *2600:*

Have you ever received any concerns or complaints regarding one of the firms/businesses that seems to be a regular advertiser in the "Marketplace" section of your *2600 Magazine - The Hacker Quarterly* publication?

I'm specifically wondering about "Hackers Home Page" at hackershomepage.com.

I discovered some negative online reviews (or feedback) on them, but wondered if you could provide any further insight. I'm a potential customer who simply wondered about their reputation for delivering "as described" functioning products.

X

You're best off asking for clarification from wherever you saw negative reviews. Sometimes there are good reasons behind them and other times they're the work of a single person with an agenda. We've never received a complaint for this particular advertiser.

Dear *2600:*

Very interesting.

You got some damn nut sitting in a prison cell, running at least two issues of this amazingly *stupid* ad. You people did not know this was an address of a federal prison?

I know you are not responsible for the ads themselves. But come on. A publication like yours running ads by inmates sitting in prison? Are you kidding me?

F

It may surprise you to learn that people in prison are as human as the rest of us. We've had members of our own staff wind up imprisoned and know of many more, often some of the brightest and most trustworthy people we've encountered. We can't speak for everyone, obviously, nor can we speak for everyone walking around on the outside. But what we can say is that everyone has the right to communicate, to read, and to write. So we're sorry if it bothers you that prisoners are afforded that opportunity by us, but nobody says you have to converse with them. In this case, the address is clearly that of a prison (state, not federal as you say), and we remind people in every issue that we make no guarantees to the "honesty, righteousness, sanity, etc." of anyone advertising in the Marketplace. This should apply when talking to any stranger and it's relatively simple to look online for anything that might concern you. It's also a good idea to be able to keep your own identity somewhat private through the use of mail drops or post office boxes. But please get past your preconceptions that everyone in prison is a "nut" that should be isolated and ignored. You will be the poorer for it otherwise.

Dear *2600:*

I am wondering if there is a place in the magazine to place classified ads? If so, how do I go about placing ads and what is the cost? I work with an inmate and he is under the impression that you place classifieds. Can you please confirm? Thanks.

Christy

What an interesting coincidence. We were just talking about this! Yes, in fact, you can place classified ads in our publication no matter what kind of room you find yourself in. But there is one condition. You have to be a subscriber. If you're a paper subscriber, simply email us (marketplace@2600.com) your subscriber number that is found on your mailing label. If you're an online subscriber, email us a receipt either from our store or elsewhere to demonstrate this. You can also send these items to our postal address which can be found on page 65.

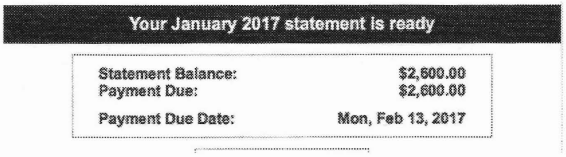
Observation

Dear *2600:*

It's been ages since I've leafed through the pages of *2600*, but I have many fond memories of both it and the various HOPEs I've attended over the years.

Anyway... I just received my credit card statement for January 2017 and *had* to pass along a screenshot because you popped into my mind instantly. I'm still chuckling - not just because it's an "even/round number" (how rare is that?) but because of the number itself (even rarer, but more special). Pretty cool, either way. Wondering if I should play the lottery next.

rick



There is actually a third remarkable element to all of this. Yes, it's rare to get a round number on a bill like that and particularly rare for it to be our name. But for it to happen to someone who is familiar with our magazine makes it even more incredible.

If anyone else out there would like to experience this on their own credit card, simply buy ten lifetime subscriptions and nothing else and you too will see $2600.00 on your bill.

Further Info

Dear *2600:*

I just came across a documentary on Netflix that I think would be of interest to other *2600* readers. The title is *Genius On Hold*. It's about an inventor/hacker named Walter Shaw. Walter worked for Ma Bell in the 1950s, starting out as a lineman and working his way up to engineer, and eventually a project manager. He had just one bad trait: he kept on making prototypes that improved their products or added new features to the services they provided to the telecommunication-starved public. Being a monopoly, Ma Bell's management wasn't very interested in touch tone phones (I'll get to that later) or conference calling, etc. "No, we make dial telephones that we lease to our customers on a monthly basis, and charge them for each one in the house." (Substitute tabletop cable boxes in 2017 to bring this story up to date.) "We happen to like things just as they are." "Thank you very much, Walter. Dismissed." Walter's innovative spirit would not be denied. He continued to make prototypes in his garage. Unfortunately, because of Ma Bell's monopoly, any device that connected to their wires, i.e., network, needed approval or was illegal. So nothing was ever approved. Needless to say, they would sue the pants off anyone who dared make improvements. Poor Walter, the once valued employee ended up with the short end of the stick again.

At wit's end and desperate to take care of his family, Walter used his skill set to make money. I won't ruin the story for everyone, but organized crime and bookies with a little unauthorized call forwarding hardware... you get the picture. Did I mention an FBI investigation and hardware sealed in epoxy with identifying marking removed? The FBI was very frustrated. Big money equals big problems for Walter again, as Bobby Kennedy "The Attorney General" decides to take on the mob. In the end, Walter is now under surveillance by his former employer Ma Bell. Walter is "testing" his remote dialing box (I told you I'd get back to it) and is arrested for making four unpaid phone calls. His sentence is four years. Ouch. In the movie, they depict the remote dialing device (it is decidedly unblue), but maybe, just maybe, we are looking at a piece of history. I for one would like to think so.

Just a small postscript. I don't want to be accused of trying to start another Oprah book club, but other members have mentioned books that I would never have found on my own. Here is one of my picks: *Turing's Cathedral* by George Dyson. Let's just say this book starts telling the history of computers and computer science just after "God Said Let There Be Light." It can be found at Amazon. I hope at least a few of you will be entertained. Thank you for your time.

Wolfgang_Von_Stinkbutt

Thanks for the pointers. We're always interested in hearing about books, films, and TV shows that speak to our audience. Let's keep the recommendations coming in.

Dear *2600:*

Hi friends,

We decided to share our book *Apoc@lypse: The End of Antivirus* for free to all. It's available for download in English and Brazilian Portuguese.

Rodrigo Ruiz

You can find this book from one of our writers on the Kindle and in PDF form on various sites throughout the net. We appreciate it being made available.

Dear *2600:*

Being behind bars gives me ample time to discover new authors. One such author is Daniel Suarez, who wrote a thrilling two-book series of tech-fiction that seems to put forth the question: "what if the game world and the real world merged?"

Daemon by Daniel Suarez follows a few characters through an adventure of epic proportion brought on by the death of an eccentric game developer. The death of this famous game developer triggers the activation of a daemon that he created, one that will spread across the entire Internet and possesses artificial intelligence. Throughout the story, this software representation of the dead programmer leads the characters on missions of discovery that take them deeper into the world of the Daemon.

One character who first discovers the presence of the Daemon on a popular game dubbed "Over the Rhine" must pass a basic test of cracking a WEP encrypted network to prove his skills to the Daemon. Another rather enterprising character gets consumed by the hunt for the Daemon. The Daemon even orchestrates the release of a convicted felon from a call center operated behind bars.

In addition to the stories of the characters, there is an excellent use of technology employed in different ways to truly distinguish this story in the realm of tech-fiction. The author expertly uses technology in highly creative ways to enhance the story, hacking together hardware and software into amazing feats of technology that seem not only plausible but not too far down the road. Just imagine for a moment if one of Google's autonomous cars decided to go on a killing spree. This type of idea and more are combined to make this story feel like it could happen in the near future - and it just might.

I discovered this book in a prison library while I looked for technology-related fiction. Once I started, I could not put it down. I read the whole

book in about 36 hours. The concluding book is called *Freedom*. Both books are probably available at your local library or on Amazon. I consider this book to be my all-time favorite in tech-fiction. I am purposely vague on some of the tech-related aspects of the book in this review so I don't ruin anything. That way, you can enjoy this book for yourself.

Chris Berge

More Eleventh HOPE Feedback

(Note: We thought we'd delve into our pile of feedback for The Eleventh HOPE again and feature some of the more interesting comments. Since we didn't explicitly tell writers that their words might be printed, we have omitted names.)

Dear *2600*:

Thank you guys so much for a great HOPE conference! My cousin came with me, her first HOPE and she had a great time.

The best part was of course, "Hackers Got Talent" - that was crazy - but so much fun. Definitely keep that tradition! The guy who you had burning the DVDs came in and was filming the dancing girl with his phone or something, and he got in the way of your cameras - if he has the footage, maybe you could post it up because we want to see the part when Jason Scott joined in and was dancing too. That was great.

As for other things we loved, the Segway was a lot of fun - we both tried it and enjoyed it. The talks were great, especially the groundbreaking talks like the "Torrenting a Pharmaceutical Drug," "LinkNYC," the updated Steve Rambam talk, the TOOOL guys, "Women in Cyber Security," and so many others.

We were a little disappointed with the car hacking talk - it was very technical and dry. It would have been better if there was more of an intro talk and then this talk would be more like an "Advanced Car Hacking" or "Nitty Gritty of Car Hacking" type of thing.

I would like to see more drones/robots - those are always fun. And wearable technology and talks about wearables.

It seemed like there were more vintage computers and phones out last time, or maybe it was just that they were organized in more of a way where they were out and people could come play with them.

We watched Mitch Altman's workshop on Arduino - it was too much theory of electronics for my cousin, but I enjoyed it. Maybe have him give an actual workshop that is an intro to electronics or something first, and then people can join in for the Arduino part afterwards? A lot of people seemed to not be paying attention after a while, just playing with the kit that they had bought. But he is great as ever.

The badges were cool and we liked that there was a contest with the lanyards - however, we still don't know what the answer was to the contest or who won. I think it would be good if there was a set time when the winners would be announced and the result would be revealed - similar to when the electronic badges were used four years ago and you could hack your badge to make it do cool things, and the badges were used to track people as they walked around.

Thanks again for the great weekend!

The Eleventh HOPE Writer 10

The details on who won the lanyard contest were revealed at the closing ceremonies. As you can see from the feedback we printed in the Autumn 2016 issue, some people want more technical talks while others want less. We had a very good response to the car hacking talk but another one that was more of an introduction certainly wouldn't hurt.

Dear *2600*:

Just wanted to tell you my appreciation for a great HOPE conference! This was my first participation and I wish I had participated in the previous ones.

My problem was I was torn between listening to the talks and participating in the workshops (Python and Arduino). Soylent was a great idea. It enabled me to listen to more talks.

I work in insurance on weekdays and I hack on weekends (carpentry, Python, Raspberry Pi, 3D printing). A number of talks provided interesting information from an insurance standpoint.

I was super impressed by the patience, kindness, and open mindedness of everyone. I rarely have felt freer than that weekend. A great feeling.

I think I'd like to volunteer next time. My only suggestion: do it every year! Congratulations on a great conference.

Amitié!

The Eleventh HOPE Writer 11

It's great to hear feedback like this. As for why we don't do it every year, it's because we don't want it to become too routine. It also takes an awful lot out of a number of people. Having that year in between conferences enables us to put more work into the next one and to participate in other conferences around the world, which is where we get so many new ideas. Rest assured - the next HOPE conference will be upon us before we know it.

Dear *2600*:

Happy to provide feedback. It was my first HOPE conference, though I've been following along and watching the videos online for years. I had a great time, and visiting New York City was awesome. I'm definitely interested in attending again in the future.

Highlights for me were:

The Doctorow keynote

"How to Torrent a Pharmaceutical Drug"

"Only You Can Stop Police Surveillance - Here's How"

"The Onion Report"

"Crypto War II: Updates from the Trenches"

"National Security Letters: The Checks and Balances Aren't Strong Enough - Sometimes They're Nonexistent"

The Internet was too fast for me. I couldn't think of anything much to use up all the bandwidth.

I think my only criticism would be that it was hard to get into some of the talks, seems like you're at capacity in the main rooms. You almost really have to plan two talks in a row in the same room if you want to be sure to see the second one. I had multiple times where I watched one talk to the end and tried to switch to another room only to find it standing room only and those getting kicked out by security for blocking the fire "lanes" in the room.

All in all, thanks for the great conference, guys. I had a great time and would attend again if the stars align.

The Eleventh HOPE Writer 12

We are planning some changes for 2018 that will give us more space. Some talks will always fill up even if we rent out a coliseum. We'll keep working on it.

Dear *2600*:

I attended The Eleventh HOPE this year - it was a great event. I was there most of Friday, and all of Saturday and Sunday. I didn't have to travel that far, coming from Queens.

It was tough having really good events overlapping. Not sure how to solve this one except don't. Of course, people will disagree about what they want to see. But I skipped the keynote to do a Violent Python workshop which had a *massive* turnout. Some feedback there: the workshops were great. Sam Bowne was awesome. His Violent Python and exploit dev workshops were a great change of pace.

It was nice to be able to stream the events when space filled out, and to watch them from the mezzanine.

I participated in EFF's CTF, which was great, but not until it was almost over on Sunday. I think they would have benefited from having a bit more promotion for that event.

I wasn't able to find anyone who could give me the WPA2 password, which was upsetting. I would prefer not to transmit packets in the clear. I was wondering why we needed a huge block of public IP addresses though. Couldn't you just have natted everybody? Anyway, it was great to see how well respected the NOC was and how much work they put together to make it happen.

This was the first HOPE I have been to and overall it was awesome. I think you guys did an awesome job putting it together. The speakers were well chosen and it was just a blast. Thanks for organizing it all.

The Eleventh HOPE Writer 13

We're happy you got so much out of it. It sounds like you really sought out a bunch of interesting events and activities. There really is no way to keep talks from conflicting. Even if you just kept to a single track, it would be impossible to see everything that was presented there. This is why archiving is so important. We now all have some time to see what we missed and to come up with ideas for 2018. As for the WPA2 password, any account name and any password worked. Anyone at the InfoDesk should have been able to give you that info, as would anyone involved with the NOC. We're sorry we didn't get the word out enough on certain things. We're so busy organizing that we sometimes forget to promote ourselves sufficiently.

Dear *2600*:

Concerning the photo policy, I really don't think anyone can have any expectation of privacy at a conference like HOPE. It's effectively a public space; if anyone wanted to capture everyone, they could obviously easily conceal a camera on themselves or leave it somewhere and get photos of every person there.

To me, the policy is a net negative. In the old days, I used to shoot a lot of photos and post a writeup on my blog or on Instagram; now I rarely post anything. I also mostly don't like staged shots - I like candid shots, and the policy now basically makes them impossible.

Thanks for being so open to feedback and thanks again for such a great conference!

The Eleventh HOPE Writer 14

You've hit the nail on the head. Even though you disagree with such policies, you also live by those rules. If enough people truly believe this is unfair, then challenging them and speaking up about them is what should be done. We agree it's impossible to avoid being captured on camera in such a public space. But that doesn't mean people should be able to annoy individuals by targeting them with a camera. While being a total jerk is legal, it doesn't mean we shouldn't tell people we don't want them to act that way.

SEND US YOUR LETTER - EMAIL LETTERS@2600.COM OR DM @2600 ON TWITTER. YOU CAN ALSO WRITE TO 2600, PO BOX 99, MIDDLE ISLAND, NY 11953 USA. YOUR OPINIONS AND KNOWLEDGE MATTER!

White House Phone Numbers

Combating Terrorism:
202 456 9361

Council on Environmental Quality:
202 456 6224

Defense Policy:
202 456 9191

EOP Service Desk:
202 456 3353

Executive Clerk's Office:
202 456 2226

Executive Secretary:
202 456 9461

Lower Office of The
Press Secretary:
202 456 9570

Management and Administration:
202 456 5400

Media Affairs:
202 456 6238

National Security Council:
202 456 9491

Office of Administration
Director's Office:
202 456 2861

Office of Communications:
202 456 2777

Office of Management and Budget:
202 395 3080

Office of Political Affairs:
202 456 6257

Office of Records Management:
202 456 2240

Office of "Science" and
"Technology":
202 456 7116
202 456 4444

Office of the Vice President
(Press Office):
202 456 0373

Office of the White House Council:
202 456 2632
202 456 7900

President's Intelligence
and Advisory Board:
202 456 2352

Resource Management:
202 456 9301

Situation Room:
202 456 9431
202 456 9451
202 456 9453

Strategic Communications Office:
202 456 9271

Switchboard:
202 456 1414 < Public number
202 456 2800 < Private number
202 395 3000 < Private number

Travel Office:
202 456 2250

Vice President Operations Office:
202 456 6770

White House Operations:
202 456 2500

HOW TO IMPROVE ZONE PROTECTION IN BURGLARY ALARMS

by Cezary Jaronczyk
Cjjconsultant4@gmail.com
cjj-consultant.ca

In this article I present a novel design of a hardwired zone control panel or zone expander input of a burglary alarm, which provides an enhanced security level against compromise attack attempts or problems with the zone loop.

Burglary alarm systems in question feature zone input connections with RF sensors and hardwired sensors. Herein I review the positive and negative properties of such zone inputs and the degree of susceptibility toward a variety of attacks compromising the secured zones. A simplified schematic of a device for testing a sensor's hardwired connections against compromising attack attempts is presented.

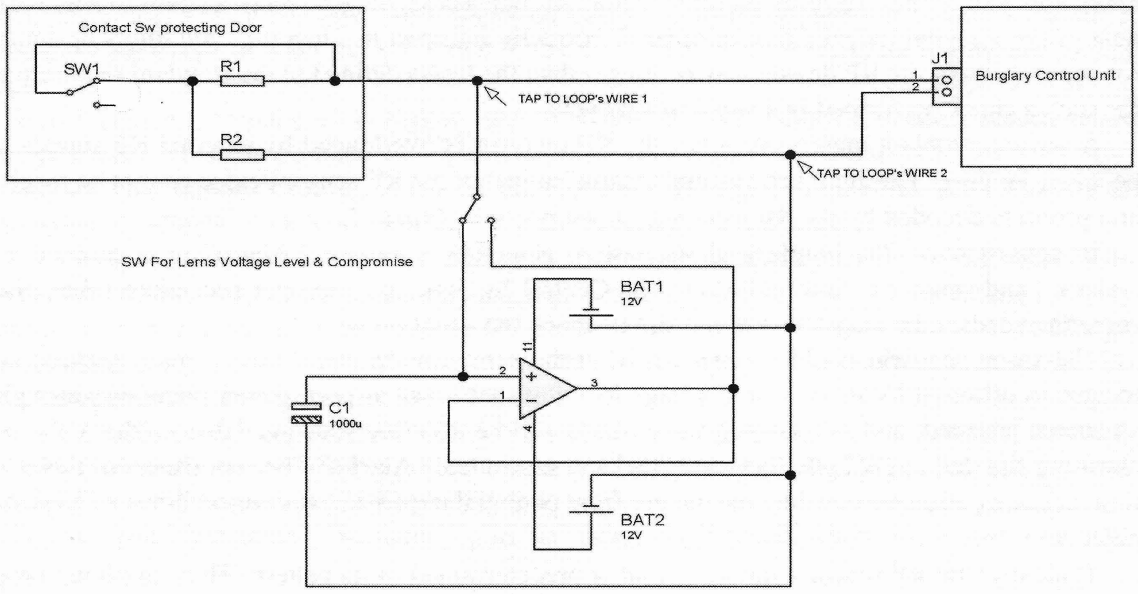


Figure 1: Simplified device used for compromising a hardwired zone loop

Do modern designs of burglary alarm systems properly and reliably protect objects or zones? This question will be answered by discussing a particular subsystem of a burglary alarm, the zone input, and its contact or switch that controls the status of a door, window, PIR (Passive Infrared Sensor), or other mechanical sensor barriers.

Modern Designs of Burglary Alarm Systems

Modern designs of the above sub-circuits provide two main technical solutions: 1) the hardwired zone inputs; 2) RF (Radio Frequency) zone input. Each of them has their advantages and weaknesses.

In the case of a hardwired zone input, the contact or switch of the sensing device, usually combined with two resistors, is connected to the zone input of the burglary control unit or to the input of the zone expander of the burglary control unit. These zone input devices can be placed at a distance of several meters apart and thus may increase the installation costs.

The activation of a contact or a switch shorts or opens one of the serial resistors and thus changes the overall loop resistance. The changes in loop resistance will cause a burglary control panel's status to change from "Normal" to "Alarm" if the burglary system is armed, or to "Trouble" when the system is disarmed.

Additionally, abnormal events, such as when the zone loop wires between contact or switch and the zone input device become shorted or cut, will also generate an "Alarm" signal.

The greatest advantage of the hardwired zone input type is that any changes of the zone loop resistance will generate adequate burglary alarm status immediately within the time limits described by the burglary alarm's system standard so that the hardwired connections are constantly supervised.

However, a serious disadvantage of the hardwired connection is that it is really easy to compromise or default the zone loop. This will be discussed below.

Compromise of the RF Type Zone Devices

The RF type zone input is an over the air type connection utilizing a sensor with a magnetic contact, or a switch like a PIR, or a door device with a built-in RF transmitter that sends its status to the RF zone receiver of the burglary control unit or the RF zone expander.

These types of connections generally are less expensive to install. However, these connections have some disadvantages.

The basic problem comes from the fact that the RF device has to periodically send a supervision signal within a maximum timeframe of a few minutes, as defined in a particular standard. When a system uses several dozen RF devices, a situation may occur when two or more RF sensors concurrently send supervisor or status change signals, and the receiver sees the messy signals and does not know how to interpret the received information. In such a case, the RF receiver needs to wait for the next cycle of signal transmission in order to correctly interpret it. Then the time limits designated for supervision of the RF device may be longer than the limits defined in the standard requirements for such a check performed in a supervision cycle.

A serious problem may occur when the RF receiver is overloaded by external RF signals and becomes jammed. During this time, the "Alarm" signal of the RF sensor device cannot be received and properly decoded by the RF receiver - it just becomes blocked.

In consequence, the burglary alarm system generates a general "Alarm" or a jammed type "Alarm" and sends this information to the Central Station, and a proper procedure takes place: someone needs to be dispatched to the site to check the situation.

The worst scenario could happen when, in the same timeframe, a few or more secured sites located in different locations - or at a large location such as an airport, power plant, or water plant - become jammed, and as a consequence, there will be no more staff available to check the next alarming site that might *actually* be attacked and send a real "Alarm." The seriousness of this situation increases when we consider the danger from potential terrorist attacks on a variety of important objects.

Typically, the RF sensor's device signal is predetermined in its pattern. Thus, applying proper RF devices and sniffing/spoofing techniques, a false substituting signal can sent with a status of "OK" right after the original RF sensor is physically destroyed. However, these compromising techniques require access to proper RF equipment and people with adequate knowledge and experience.

All of the above problems are consequences of the fact that the RF signal may be visible to anybody with appropriate devices.

Compromising Hardwired Connections

Considering all of the above, hardwired type connections seem more reliable and safe in securing a wide variety of sites. However, in order to make a hardware type connection safe, we need to solve the problem of compromising it.

Because the hardware zone loop is powered by a constant voltage level delivered by the burglary control unit or a zone expander, it is very easy to apply devices that can read and remember the voltage level in the zone loop and later, on a request, feed it back to the zone loop.

When, for example, the applied compromising voltage level represents the status of "closed door" (window or other barrier), then opening the door (window or other barrier), will not affect the zone loop voltage level because a burglary control unit sees the zone loop status as not changed. In this way someone can access a protected area without being noticed.

Figure 1 shows a simplified example of compromised devices and tactics, and a way of taping it to the zone loop wires. These types of devices allow compromising the protected zone loop for a timeframe of up to 30 minutes or even longer.

To be more precise, based on Thevenin's theorem, if an external compromising voltage equals the voltage level presented when the door is closed, and if during the compromise attack this voltage is applied to the zone loop, then opening the switch or contact that usually changes the serial zone loop resistance will have no effect on the loop parameters seen from the zone loop input terminal, as the compromising voltage compensates for the loop resistance changes.

In the case where more than two wires count in a zone loop, more compromising devices may be used to connect to the wires in a circular pattern, in order to monitor and then substitute all voltages presented in the zone loop circuits.

How to Prevent Compromise Attacks on a Hardwired Zone Loop

The case presented above is of such importance that it needs to be prevented. This can be accomplished by changing the way the zone loop is powered, from DC with a constant voltage level to a random variable voltage level constantly changing over time.

As the results of applying a random variable voltage power to the wired zone loop, as shown in Figure 2, it will be extremely difficult to successfully perform any of the above discussed compromise techniques in order to disable the protected zone.

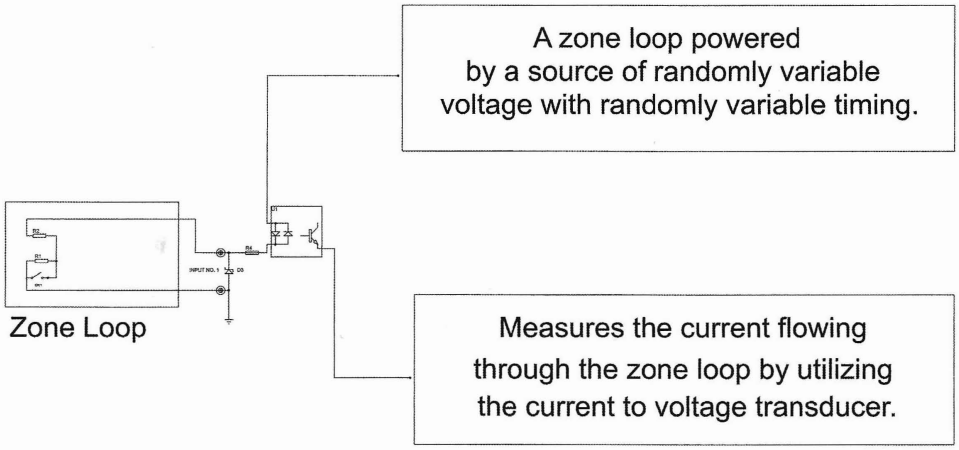


Figure 2: A wired zone loop powered by random variable voltage and timing

In practice, the easiest way to protect a hardwired zone loop would be to insert - between the zone loop and the burglary control panel - a device called a Burglary Alarm Zone Enhancer, which will power the zone loop with random variable voltage level and will process the status changes of the contact or switch and pass the result to the input of the control unit as shown in Figure 3.

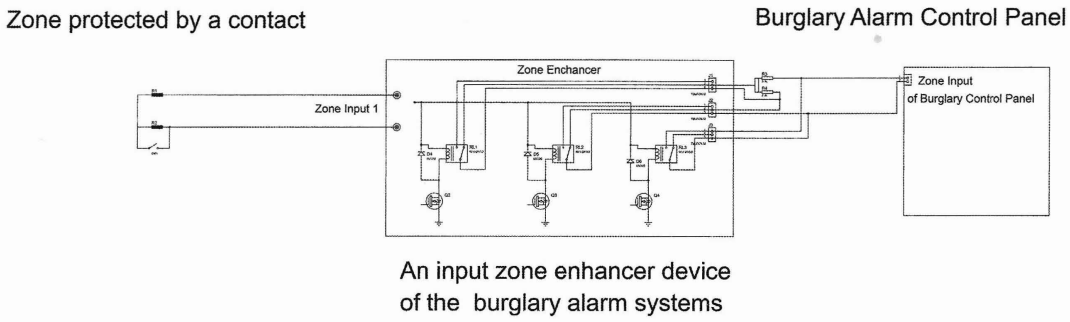
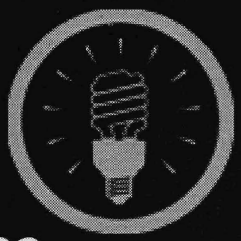


Figure 3: Burglary Alarm Zone Enhancer

The device named Burglary Alarm Zone Enhancer described above has a Patent Pending status. If you are interested in this subject, feel free to contact me.

EFFecting Digital Freedom



We're Halfway to Encrypting the Entire Web

by Gennie Gebhart

The movement to encrypt the web has reached a milestone. Mozilla recently reported that the average volume of encrypted web traffic on Firefox now surpasses the average unencrypted volume. Google Chrome's figures on HTTPS usage are consistent with that finding, showing that over 50 percent of all pages loaded are protected by HTTPS across different operating systems.

In other words, we're halfway there.

EFF and our members have been pushing for more widespread adoption of HTTPS since 2010. The Firesheep extension had just been released, and it made painfully visible what had been scaring the security community for years: just how easy it was for any network eavesdropper to take over another user's session simply by sniffing packets and copying the victim's cookie. Firesheep only worked so frighteningly well because it took advantage of websites that failed to offer encryption to their users, thus leaving them vulnerable to such trivially easy attacks.

The answer, of course, was HTTPS.

At first, we had to wait for tech giants and large content providers to lead the way in HTTPS implementation. We applauded when Facebook and Twitter implemented HTTPS by default, and when Wikipedia, Reddit, and other popular sites later followed suit. EFF's "Encrypt the Web" report played a big role in tracking and encouraging crypto best practices, and recently we have been encouraged to see other efforts like Secure the News and Pulse track HTTPS progress among news media sites and U.S. government sites respectively.

But the real HTTPS victories have come when smaller, independent websites start to make the shift. This is where Let's Encrypt and Certbot have changed the game, making what was once an expensive, technically demanding process into an easy - and free - task for webmasters across a range of resource and skill levels.

Let's Encrypt is a Certificate Authority (CA) run by the Internet Security Research Group (ISRG) and founded by EFF, Mozilla, and the University of Michigan, with Cisco and Akamai as founding sponsors. In our analysis, Let's Encrypt is the largest CA on the web. Since this past October, Let's Encrypt has exploded from 12 million active certs to over 28 million.

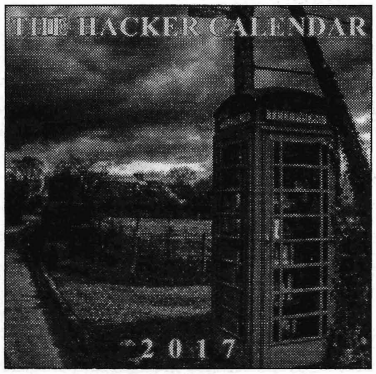
Most of Let's Encrypt's growth has come from giving previously unencrypted sites their first-ever certificates, thus paving the way for a more encrypted web. A large share of these leaps in HTTPS adoption are also thanks to major hosting companies and platforms - like WordPress.com, Squarespace, and dozens of others - integrating Let's Encrypt and providing HTTPS to their users and customers.

If you have shell access to your hosting provider, you can use EFF's Certbot tool to get a free SSL/TLS certificate from Let's Encrypt and automatically configure your Apache or Nginx server to use it. Certbot will also work with any other CAs that support the ACME protocol. While there are many other clients that implement the ACME protocol to fetch certificates, Certbot is the most extensive client and can automatically configure your webserver to start serving over HTTPS immediately. For Apache, it can also optionally automate security tasks such as tuning cipher suites and enabling important security features such as HTTP to HTTPS redirects, OCSP stapling, HSTS, and upgrade-insecure-requests.

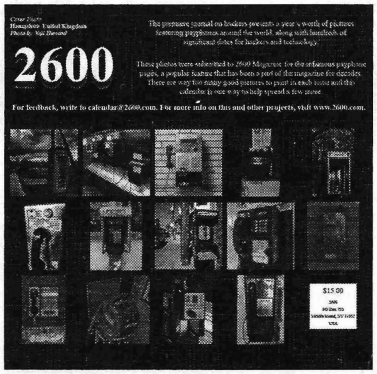
While it's good news that we are halfway to an entirely encrypted web, we still have more work to do. We need more wins like the ones we get every time a small website owner - probably just a nerd with a laptop like you and me - offers HTTPS to their users for the first time. If we want a web that is safer from eavesdropping, content hijacking, cookie stealing, and targeted censorship, we need to keep advocating for HTTPS as the default across the web.

PRICES SLASHED

We've cut our 2017 calendar prices nearly in half! 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.



Only $5.99
plus shipping
at store.2600.com



ATTENTION WRITERS

o

You now get more when you have an article published in *2600*
For each article printed, you'll receive:
One year of *2600* (subscription, back issues, paper/digital)
AND
One of our *2600* hacker t-shirts

(that "AND" used to be an "OR")

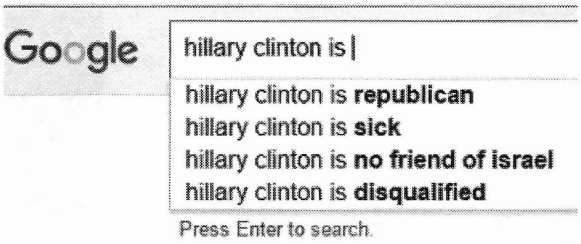
ATTENTION LIFETIME SUBSCRIBERS!

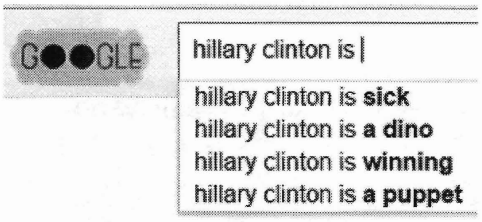
If you want to receive annual digital digests instead of - or in addition to - your quarterly paper issues, this is now possible without having to buy both at full price. For $100, we will sign you up for the lifetime digital digest plan as well (once we verify that you are an existing lifetime subscriber). You will receive all of the digests that have already been released (Volumes 1-14 and 25-32) plus five newly released ones each year, and one per year once all of the back issue digests have come out. Just visit the downloads section at store.2600.com and sign up!

Since we take the word "lifetime" quite seriously, we will not cancel your existing subscription as long as you are still living. However, if you really don't want to get paper issues anymore, simply tell us this and you can transfer your subscription to someone else on our newly created lifetime waiting list. (It's like an organ donor waiting list but a whole lot more pleasant.) And you'll feel great having donated your remaining paper issues to someone who wouldn't have gotten them otherwise. Full details can be found at our store.

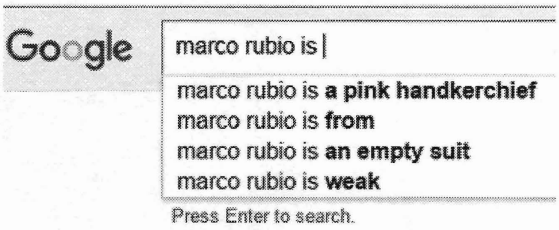
(Continued from page 21)

Hillary Clinton - Democratic presidential candidate.
The first search was performed in April 2016 while in the U.K.
The second one was performed in June 2016 while in the Netherlands.

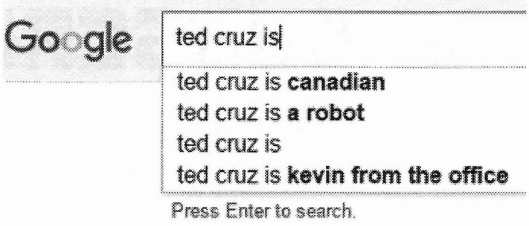


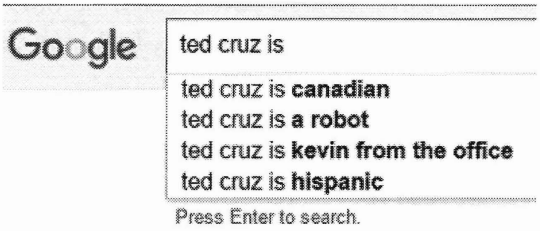


Marco Rubio - Republican presidential candidate.



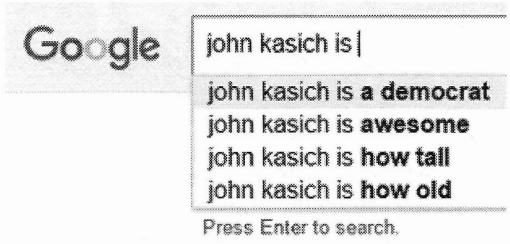
Ted Cruz - Republican presidential candidate. The first search was performed via Google UK in the U.K. The second search was performed slightly later in the Netherlands but also via Google UK.

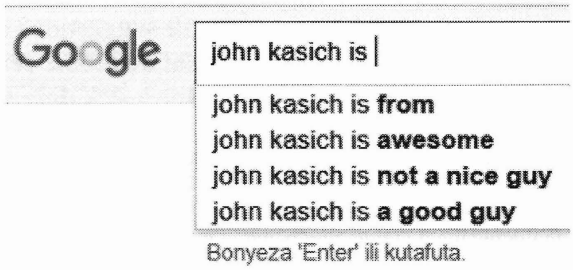




It appears there is a possibility, per the Internet, that Ted Cruz is a Canadian/Hispanic robot who secretly leads a double life as the actor Kevin Malone. I could envision a movie based on this premise.

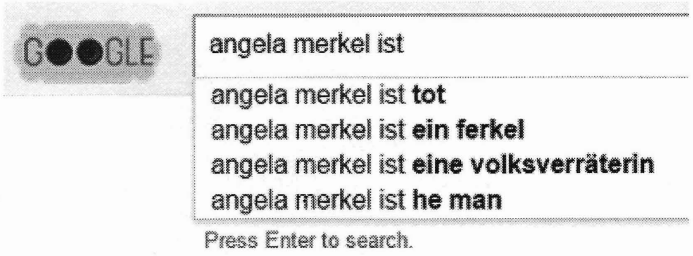
John Kasich - Republican presidential candidate. The first search was performed early in the campaign. The second search was performed in East Africa after he was out of the race.





Germany

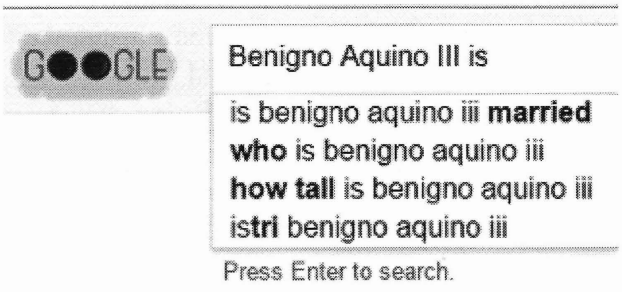
Angela Merkel - Chancellor of Germany



"Tot" means dead. "Ein ferkel" means a piglet. I'm not 100 percent on "eine volksverräterin" but I think it deals with the anti-immigration movement in the European Union. "He man" is most likely saying Merkel is a man, or perhaps He-Man has a lot of fans in Germany. They still love David Hasselhoff. I prefer to think He-Man; it's just cooler.

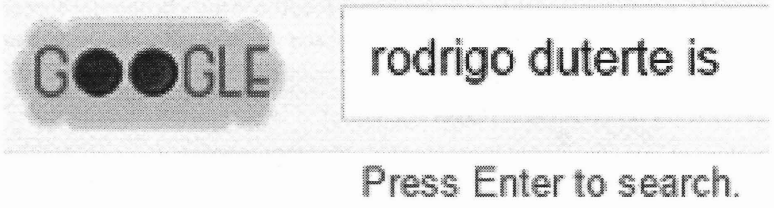
Philippines

Benigno Aquino III - Outgoing President of the Philippines



"Istri" per Google Translate means ironing, but I can't figure out the context. Height and marital status seem to be an important factor mentioned in other examples.

Rodrigo Duterte - Newly elected President of the Philippines



Apparently nada exciting in auto-fill. Not that unusual. Many lesser known offices and candidates came up blank with this search term, but others had funny results.

Could an undecided voter be influenced by the auto-fill suggestion? Could potential voters be swayed by the inference? Does Bernie Sanders, a potential awesome serial killer who's out from nothing have a chance against: Hillary Clinton who could be a sick dino winning puppet versus the best awesome dead liberal candidate Donald Trump?

Although I find the results funny, there is manipulation going on, bot or people. Most if not all search engines are vulnerable to some sort of search manipulation. Google is not unique. In an ideal world, results would come with a basic warning: "The results returned are not necessarily 100 percent accurate and many have been enhanced for marketing purposes."

Have fun seeing what you can return from auto-fill. My favorites are Putin, Erdogan, and Bob Ross. But please don't vote based only on the auto-fill suggestions, no matter how cool it sounds to elect robots or dinos as President.

"The Stag Lane Engine Assembly Shop" by Robert Cutts is licensed under CC BY 2.0

by Malvineous

In issue 33:1, there was an interesting article by Ben Kenobi detailing a method for checksumming files on a system to discover any unauthorized modifications. This got me thinking - if presented with a system like this, how might one find their way around this seemingly impenetrable layer of security?

The system produces a signed list of all important files, complete with a checksum for each one. The idea being that should any file be tampered with, its checksum will change so it won't match the list, and the intrusion is detected.

Updating the master list requires some work - creating new keys, comparing changes to the old list, etc. - so let's imagine that due to this effort, security updates aren't applied as often as they should be. Someone breaks into the system and uses a recent vulnerability to gain root access. This part is not that unusual, which is the reason why one might go to the trouble of having the checksum list in the first place.

Now, most intruders might install a script somewhere and have it run at boot time. This script could be installed anywhere, and if it's placed in an unmonitored directory (say deep within ~/.config/) then the checksum process will not pick it up, as it is avoiding those directories to minimize false positives. The script can be marked as suid root so that it will always run as root (even if launched by a normal user later on).

Loading it at startup can also be quite straightforward - just put it in the user's own startup scripts, such as ~/.Xsession, ~/.bashrc, or similar.

This means that despite all the elaborate checksum tests, it's still possible for a malicious program to run unnoticed on every boot, with full root privileges.

Taking it a step further, once our malicious program is running, perhaps we might want to capture some passwords or private keys. One way of doing this is to replace the PGP binaries with our own modified versions, which have been changed such that any time a private key passphrase is entered, the passphrase along with the key is sent to a remote server - possibly via a series of specially coded DNS lookups so as to avoid creating any unusual-looking outgoing network connections.

Once we replace the PGP binary on the system with our malicious version, we can capture any private keys and use them ourselves to decrypt whatever we need - at least until the next checksum run, when the user will realize that /usr/bin/gpg or similar has been modified.

However, if we have looked around the system and discovered this checksum process, we will see that it is using the sha256 program to produce the checksums. Depending on the system, this means we can either replace sha256 itself or one of the libraries it uses to calculate the checksums (such as OpenSSL), so that we can control the checksums produced. A few simple lines of code at the right place ("if checksum = A then checksum = B") means that any time the "wrong" checksum is calculated, it will be replaced with the "right" one and all our modified programs will still show up as having their original checksums, appearing as though they have never been changed.

As a side note, this illustrates one of the dangers of relying on in-band security - where you are using a system to verify itself. If the system has indeed been compromised, then you can no longer trust the verification process as it too could have been tampered with. If you can't trust that the verification process is telling the truth, how do you know whether the system has been compromised or not?

Getting back to our malicious programs, you might think booting off read-only media will prevent programs from being replaced. Many systems that can boot off read-only media have the ability to mount overlay filesystems to give the impression that the filesystem is read-write. It would not be that difficult for the suid binary to run in the user's own startup scripts, then, as the root user, mount a new overlay filesystem with the modified sha256 and PGP binaries overriding the originals. It would do this on every boot, which means if you examined your boot media on another running system it would look fine, and if you booted a machine with it and ran the checksums there, it would still look fine - even though it was sending all your passwords out to a remote system.

Admittedly there are many ifs and buts in this scenario, and you could argue that if you are targeted individually then there is little you can do anyway. However, when discussing security I always find it interesting to think about how one might get around it, as it can often lead to ideas that make the system more secure - for example, much of this scenario could be defeated (or at least made more difficult) by setting the read-only boot media to mount the home directory and other read-write areas with the "nosuid" option, so they cannot run suid binaries.

There is actually nothing wrong with this idea of checksumming your files - in fact there are a number of IDS (intrusion detection) programs out there that will do it for you automatically. Many attacks are of the "smash and grab" variety that won't try very hard to defeat an IDS anyway, so checksums actually work quite well. As with any type of security, the issues only arise when you put your complete trust in an idea, or it's your only line of defense.

So my thanks go to Ben Kenobi for the thought-provoking article, and for making me discover that even though I don't use checksumming on my own system, I probably should still be mounting my home directory with the nosuid option!

Thoughts on Phoenix Project II

by GI_Jack

Regarding "Hacking For Knowledge" in 33:3, I'm somewhat amused by your little project. It's cute, and I fondly remember running similar setups as a teenager. As a man who's been running home servers up until I started working in data centers and hosting my own professionally, I'll give you a hand.

OS Choice

What year was this written in? Ubuntu 12.04 is ancient and outdated. The latest LTS is 16.04, which, if you go the Ubuntu route, is your choice. The older the distro, the sooner it goes into unsupported. But I'll elaborate.

You have three decent choices for Server OS: Debian, Ubuntu *Server,* and CentOS (or RHEL). Fer fawks sake, don't run a desktop version on a server. If you don't know how to use ssh, learn.

Also, use the 64-bit version. To reiterate, Ubuntu Server 64-bit version.

Hardware

32-bit hardware is a no-go. There is no reason to throw a 2GB RAM 32-bit Celeron back into service. You can get a Dell PowerEdge 1950 for $20 on eBay, and you can get Dell workstations with similar electronics for about $50 that don't require a rack mount. Parts are also cheap, so you can find OEM RAID cards and power supplies cheaper than you can desktops. I recently paid $10 free shipping for a second power supply for a 1950.

Servers in the modern day should be 64-bit and run 64-bit OSes. They should also be multi-core. The workstation motherboards are good because you can shoehorn multiple Xeon CPUs, and they have lots of slots for RAM. 32 GB of RAM with eight cores on two CPUs is not entirely unreasonable at $25 for everything.

Also, when you get server grade shit, XEONs have larger cache and the mobos support ECC FB RAM. Coolness.

RAID. If you want to host a server, you need RAID. At the very least, RAID-1 mirroring. RAID-1 mirrors two disks, so when one of them fails, it can be replaced without interruption. If you are using a rackmount, you likely have a quick release sled where you can quickly replace failed hard disks with no downtime or loss in service. RAID-1 is the gold standard for "production" servers. There are two types: hardware and software.

Software

Apache is not bad. Investigate NGINX and PHP-FPM as an alternative - faster and exploited less often.

ownCloud as alternative groupware. Combine with Postfix and Dovecot to use email.

ownCloud has integration with Android and GNOME Shell. I use this ownCloud/Postfix/Dovecot stack as the integral part of my vertical Linux stack which includes GNOME desktops and Android cell phones.

MS Exchange is great, but in the Linux world, it's not what we need.

Also, ditch the FTP server. It's unencrypted and, in today's world, that means some asshole like Jack over here is going to snarf your shit and then make fun of your porn habits, just for laughs. SSH comes with SFTP, so use that as much as possible. SFTP is used just like FTP, except it runs over SSH. All major FTP clients support SFTP.

Management

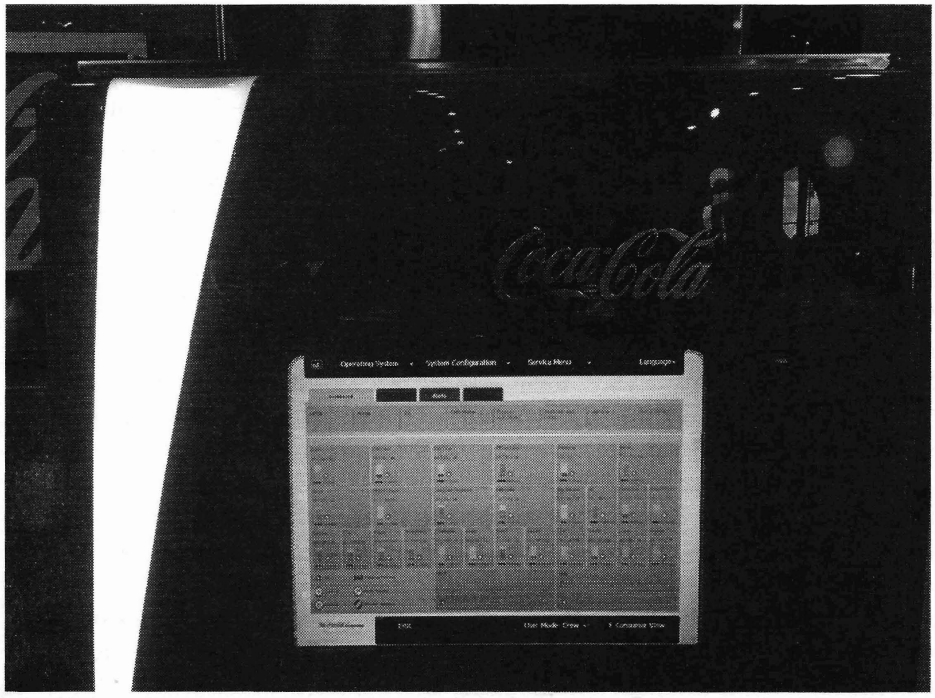
Alrighty, because we don't want to get SSH popped by some skid, we need a management interface. For this I use OpenVPN as a management network and SSH and all consoles face the VPN IP. Hidden from the outside world. I also use a certificate chain with RSA certs and TLS packet encryption, which makes it hard to bruteforce/recover the key, and packet encryption with a combination of using UDP packets means that the server will not respond unless the packet is correctly encrypted. Therefore, my OpenVPN setup cannot be detected with Nmap or other port scanners.

So, best of luck to your "Phoenix Project." I had to rewrite this a few times to get the expletives out. I also tried to keep it brief, as it'd take another ten pages to give examples of everything. $SEARCH_ENGINE is your friend here.

THOSE COCA COLA FREESTYLE MACHINES IN CREW MODE

by M0ebiusStrip

I happened upon this Coca Cola Freestyle machine at a local Zaxby's Chicken restaurant. One of the employees accidentally left it in "Crew" mode after making an adjustment. As you can see, the touch-screen gives a graphical overview of syrup levels, temperatures, and the menu folder options, allowing the operator to view Errors, Alerts, and Notices. Touching the bottom-right corner of the interface returned the machine to regular "Consumer" operating mode. Touching there again returned me to "Crew" mode - without needing a password. I share this in the spirit of exploration and curiosity. I took these pictures with my own phone, right before the manager on duty came over and said "Having trouble getting your beverage?"



"No, thanks," I replied "The machine was in 'Crew' mode and I'm just a curious person - always wondered how these things worked."

He was really friendly, and replied "This is just the business end. The real party is in the back, where all the syrup tanks and compressors live! I'd show you, but our insurance doesn't let non-employees behind the line."

More people should be like that guy!

321 Studios Revisited

by Nordog

Back in the day at 3 Research Park in St. Charles, Missouri, things were buzzing, along with the tail rotor of the boss's private helicopter. Robert H. Moore had us all helping to promote the freedom to duplicate your own copies of DVDs, placing him in the middle of the digital age's most volatile disputes between consumers' fair rights and the MPAA's views of copyright protection.

In October 1999, DeCSS was created, which allowed Pandora out of the DVD box set. We all had a right to rip our own copies of DVDs we had paid for - movies, records, and video game content. In July 2001, Bob just took this idea and ran with it. Thus, DVD X Copy was born. It all started on Edison Avenue in Chesterfield with a bunch of young hungry people with an idea: create software that allowed everyday people to make backup copies of their DVDs. It was fun and a lot of work; there were a lot of great ideas that started in that little building. X Maker, CD X Rescue, Xtreme Download, X Show, X Copy Platinum, and X Point were just a few. We had computer parts and software spread everywhere. What a great atmosphere - free lunches for everybody and a free spirit encompassed the entire enterprise. No rules, just do it ("Now You Can" - our motto till the end). Even our passwords reflected that freedom, aka. 321 Geeks ruled. We were on AfterDawn, BBS's, and IMing everybody, downloads were flying on every system way before the thought of any aviation vehicles were on our bosses' minds. We were making money and loving life itself. Oh to be young again.

Soon we had outgrown that little space and were on the move - in more ways than one. One was the lawsuit. Let's file a lawsuit against Hollywood and where else but northern California. We started including anti-piracy measures in the software, watermarks, and disclaimers, even not allowing the copy to be copied.

Our next move was to 17 Research Park and a much bigger building with a big United States flag in front of the campus. Things were getting more serious, you had to sign for things like DVD burners, hard drives, motherboards, meals, office supplies, you name it - and it all had a price and had to be accounted for. We had the first Power Users Conference on Saturday, August 30, 2003 and what a showing... even Fred von Lohmann offered advice in a speech for the masses. There were suits and ties for the first time and everybody started getting official titles and salaries. A call center was in the making and 24/7 operation all a part of doing *big* business.

Las Vegas, January 8, 2004: Three new products and the start of the end. All the new leaders went to Nevada. Bob even flew the helicopter for a while at least, everyone else just took a plane. The rest of the old guard had to rely on AfterDawn and IMs that weekend. But there was a holiday party coming up and it was on the company's tab, a "Let's celebrate the success and the People of 321" gala, January 24, 2004. Elegant Dress for an evening at the Omni Majestic Hotel in downtown St. Louis. Dancing, dining, and a lot of whining - where had we gone, what had happened? There were tuxedoes, evening gowns, and fine linen. Gold was everywhere - a lot of snobby people and very little enjoyment. Some of us had to go to work the next morning and there was an ice storm in St. Louis that night. There was a change in the air - little did we know, we were on the move again. Bigger is not always better.

3 Research Park Drive and the Tower of Glass. More changes and staffing moves were rampant - even Bob's son quit. It all came down to production. Everyone was asked to work overtime to help the production software assembly line make more, more, more. There were more changes in the wind, a lot of new faces started to show up, and things really changed fast. There were logical paths and steps for everything, Human Resources reared its ugly head, you had to tell where you were going and clock in and out. The smokers had to go outside and it is really cold in Missouri in the winter. What was happening? Our very freedom was being taken away. An employee handbook was even issued in February. I saw the writing on the stall wall.

Then, on February 20, 2004, Judge Susan Illston ruled. Wow, what a change and not for the better of anyone. Even though Mr. Moore said he would fight to the end, on June 16, 2004, he started preparing for bankruptcy protection. $100 million dollars a year in revenue and 400 employees later, it was all over. But boy, what a ride. 321 Studios is gone but not forgotten. Long live the idea.

Now you can.

In memory of Robert H. Moore, who passed away April 1, 2007

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.

April 14-17
Easterhegg 2017
Willy-Brandt-Halle
Mühlheim am Main, Germany
eh17.easterhegg.eu

April 22-23
Maker Faire Chicago
McCormick Place
Chicago, Illinois
www.makerfaire.com/chicago

May 4-5
THOTCON 0x8
Chicago, Illinois
thotcon.org

May 19-21
Maker Faire Bay Area
San Mateo Event Center
San Mateo, California
www.makerfaire.com/bay-area

May 19-21
NolaCon
Crowne Plaza New Orleans French Quarter
New Orleans, Louisiana
nolacon.com

May 25-28
GPN17
Karlsruhe, Germany
entropia.de/GPN17:Barrierefreiheit

June 8-9
RVAsec
Virginia Commonwealth University
Richmond, Virginia
rvasec.com

June 9-11
CircleCityCon 4
Sheraton City Centre
Indianapolis, Indiana
circlecitycon.com

June 24-25
Nuit Du Hack
Disneyland Paris Convention Center
Paris, France
www.nuitduhack.com

July 27-30
DEF CON 25
Caesar's Palace
Las Vegas, Nevada
www.defcon.org

August 4-8
SHA2017 Hacker Camp
The Scoutinglandgoed
Zeewolde, The Netherlands
sha2017.org

September 22-24
DerbyCon
Hyatt Regency
Louisville, Kentucky
www.derbycon.com

September 23-24
World Maker Faire New York
New York Hall of Science
Queens, New York
www.makerfaire.com/new-york

October 26-27
GrrCON
DeVos Place
Grand Rapids, Michigan
www.grrcon.org

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

Marketplace

For Sale

PUT A SWISS BANK IN YOUR POCKET. http://cryptobiz.directory offers financial freedom, profile page, email address, and phone number with voice mail on a pay-as-you-go basis. Secured with Open Source software and hosted in a converted Swiss bunker deep inside a mountain.

BLUETOOTH SEARCH FOR ANDROID searches for nearby discoverable Bluetooth devices. Runs in the background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and manufacturer. Handles Bluetooth Classic and Bluetooth LE (on LE-equipped Android devices). This is a valuable tool for anyone developing Bluetooth software, security auditors looking for potentially vulnerable devices, or anyone who's just curious about the Bluetooth devices in their midst. Exports device data to a CSV file for use in other programs, databases, etc. If you've used tools like btscanner, SpoofTooph, Harald Scan, or Bluelog on other platforms, you need Bluetooth Search on your Android device. More info and download at http://tinyurl.com/btscan.

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.

NEEDFULWARES.COM. Thank you for your time today in reading this. Please visit this site to view the most beautifully hacked coins and hardcover books, handmade in the still-great USA! There are wonderfully handcrafted (some may called them hacked) coin rings (and book safes to hide them in) for EVERYONE. Yes, I make change into something you can wear on your body and books that will keep your wares (or whatever) safely hidden. These are great gift ideas and all my work has a Made-In-USA, money-back, no-hassle guarantee. Custom, handmade by myself, orders are available.

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

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. WINTER EDITION now available!

A TOOL TO TALK TO CHIPS. It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only $30 including world wide shipping. Check out this open source project and more at DangerousPrototypes.com.

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, poker cheating equipment, computer devices, odometer programmers, and much more. www.hackershomepage.com

HACKERSTICKERS.COM has added tons of new shirts and lock picks for hackers, programmer and security geeks. Get a free sticker with purchase, just add to cart and enter "freestick" at checkout.

PRIVACYSCAN seeks & destroys privacy threats on the Mac wiping your tracks on where you surf and what you do on your computer. Learn more at http://privacyscan.securemac.com/

Announcements

HAVE YOU SEEN THE NEW *2600* STORE? We've finally made the jump into the 21st century with a store that has more features, hacker stuff, and endless possibilities than ever before. We now accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. We have more 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

COVERTACTIONS.COM is the place to find encryption products from around the world. Search by type, country, open source, platform, and more. Over 860 products listed with more added every day. Suggestions and feedback welcome.

SECUREMAC.COM IS BACK with the latest Apple security news! Submit your articles, writeup, and advisories. MacScan 3 was just released as well offering anti-malware protection for Mac OS X. Visit SecureMac.com.

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

SPIRENT FEDERAL SECURITY TESTING. Spirent Federal SecurityLab services are structured to produce high-impact results with minimal impact on the client organization. Our dedicated teams of experienced security professionals offer comprehensive scanning, cryptographic analyses, penetration testing and monitoring services for networks, wireless, websites, mobile applications, embedded devices, as well as source code analysis. Contact us today to learn more at 801-785-1448 or securitylabs@spirentfederal.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, 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.

LISTEN TO THE GREYNOI.SE PODCAST. There are many information security podcasts out there, and we're just one of them. We are here for the newbies and veterans alike! The greynoi.se podcast discusses general news, science, and privacy as well as technology specific issues, all from the hacker perspective. Recorded LIVE at the SYNShop Hackerspace in Las Vegas, NV, Friday nights at 7 pm. Recorded shows are usually online by Monday evenings. Have a listen and we LOVE feedback! https://greynoi.se

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.

SECURE UNIX SHELLS & HOSTING SINCE 1999. JEAH.NET is one of the oldest and most trusted for fast, stable shell accounts. We provide hundreds of vhost domains for IRC and email, the latest popular *nix programs, access to classic shell programs and compilers. JEAH.NET proudly hosts eggdrop, BNC, IRCD, and web sites w/SQL. *2600* readers' setup fees are always waived. BTW: FYNE.COM (our sister co.) offers free DNS hosting and WHOIS privacy for $3.50 with all domains registered or transferred in!

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 simply respond with one liners from *50 Shades*. We accept Bitcoin and promote encrypted registration over Telegram Messenger. Use promo code COSBYSWEATER2600 for 50% off (https://www.doublehop.me).

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/

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMES? Stand up for your rights! Be polite, respectful, and calm. Repeat your own version of the following mantra: "Officer, I respectfully invoke all of my legal and Constitutional rights. Based on advice of counsel, I respectfully request to talk to my lawyer, I want to remain silent, and I will not consent to any search or seizure. Am I under arrest? Am I free to leave? Can I go now?" Omar Figueroa is an aggressive Constitutional and criminal defense lawyer with experience representing persons accused of hacking, cracking, misappropriation of trade secrets, and other cybercrimes. Omar is a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and for more than a decade has provided pro bono representation for hackers, whistleblowers, and 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 (protester allegedly connected with Anonymous involved in a DDOS action against PayPal and member of the PayPal 14). Also, given that the worlds of the hacker and the cannabis connoisseur have often intersected historically, please note that Omar also defends non-violent human beings accused of committing cannabis offenses and also helps his clients understand the complex maze of medical marijuana-related laws and regulations in California. Please contact Omar Figueroa at (415) 489-0420 or (707) 829-0215, at omar@alumni.stanford.edu, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472.

FBI FILES - Public service websites GetGrandpasFBIfile.com and GetMyFBIfile.com provide simple form letters to get dossiers from the FBI and other agencies. Free of charge. You can also print out the blank request templates if you prefer not to share personal information while using the website.

ANTIQUE 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

DATA RAIN SOLUTIONS is a budding Colorado IT startup specializing in reliable and affordable remote tech support in advanced malware removal, PC optimization, diagnostics, and more. *2600* subscribers get 10% off their first order, as-need basis, or 1 year sub. Contact us: shanaroneasomi@yahoo.com. Visit us: http://shanaroneasomi.wix.com/datarain. Join the team! (Hackers welcome)

HACKERS, PHREAKERS, COMPUTER NERDS. Feel disillusioned, depressed, and dissatisfied with the way your life is passing? Need love, happiness, togetherness, and financial freedom? Here is the solution. Be with us to be yourself. You can be independent by joining with your kind. Enjoy the possibilities of collective thought, with associates who feel and think just like you do. Break that old routine, and dare to explore something new and unique. Contact THE HUB at: P. Bronson, P.O. Box 1000-AF8163, Houtzdale, PA 16698-1000.

Personal

OPERATION PRISON PIRATE needs your help! OPP Media started as a hobby in 2012 to provide uncensored information and entertainment to various prisons in the U.S., but we've hit the limit of what we can do by ourselves. We really need donations. It costs us about $50 per broadcast, all out of pocket. Recently, our main transmitted was damaged, and we can't afford to replace it. We are also looking for engineers, producers, voiceover talent, or anyone who can help us in any way. We'd like to expand to cover even more prisons, but we need some help. E-mail us at OPPmedia@hushmail.com, and send bitcoins to 1J34tpXw84qM39LEZRtnUiVVpmuU6oxQJE.

GOT TORPEDOED OUT OF THE FREE WORLD. Living in Fed world now, but would like to stay up on infosec, surveillance, and government oppression. I have written white papers on 4th Amendment issues, and would love like-minded people to correspond with and receive articles from. Kevin Reynolds, 59650-018, FCC Coleman-LOW, P.O. Box 1031, Coleman, FL 33521.

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 Summer issue: 5/21/17.

"Hacking is bad and it shouldn't be done. But look at the things that were hacked. Look at what was learned from that hacking."
- President-elect Donald Trump, January 11, 2017

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

STAFF

Infrastructure
flyko

Network Operations
phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Invisibl Skratch Piklz, Philip Glass, Kendall Morse, Linton Kwesi Johnson, YG

Shout Outs: Kitten Academy, The Font Family, WUSB 2.0, The Resistance Manual, indivisibleguide.com

***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); Spring 2016, Volume 34 Issue 1, 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 - $27 individual,
$50 corporate (U.S. Funds)
Overseas - $38 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2015 are $27 per year or $6.95 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**

MEETINGS

ARGENTINA

Buenos Aires: Bodegon Bellagamba, Carlos Calvo 614, San Telmo. In the back, tables passing bathrooms.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4199, Capital Federal. 7 pm

AUSTRALIA

Central Coast: Gurimbah RSL (in the TAB area), 6/22 Pacific Hwy. 6 pm.
Melbourne: Oxford Scholar Hotel, 427 Swanston St.
Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

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

Cannes: Palais des Festivals & des Congres la Croisette on the left side.
Grenoble: EVE performance hall on the campus of Saint Martin d'Heres. 6 pm
Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm
Paris: Burger King, first floor, Place de la Republique. 6 pm
Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm
Rouen: Place de la Cathedrale, benches to the right. 8 pm
Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 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

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
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 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

RUSSIA

Moscow: Pub Lora Craft, Pokrovka St 1/13/6. 7 pm

SWEDEN

Stockholm: Starbucks 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

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm
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: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

Scotland

Edinburgh: Rose St, between 1780 and Dirty Dick's.
Glasgow: Starbucks, 9 Exchange Pl. 6 pm

Wales

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

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

Arizona

Phoenix (Mesa): HeatSync Labs, 140 W Main St. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm
Tucson: Sunny Daze Cafe. 6 pm

Arkansas

Ft. Smith: River City Deli at 7320 Rogers Ave. 6 pm

California

Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (business park behind the thrift store). 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
Sacramento: Hacker Lab, 1715 I St.
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

Newington: Panera Bread, 3120 Berlin Tpke. 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
Titusville: Bar IX, 317 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. Payphones: (208) 342-9700.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Space by Doejo, 444 N Wabash, 5th floor. 6 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 Bitting 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: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

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): Las Vegas Hackerspace, 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: Cup A Joe, 3100 Hillsborough 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: Emma Inc., 11 Lea Ave. 6 pm

Texas

Austin: The Chicon Collective, 301 Chicon St, Suite D. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm
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
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington

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

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

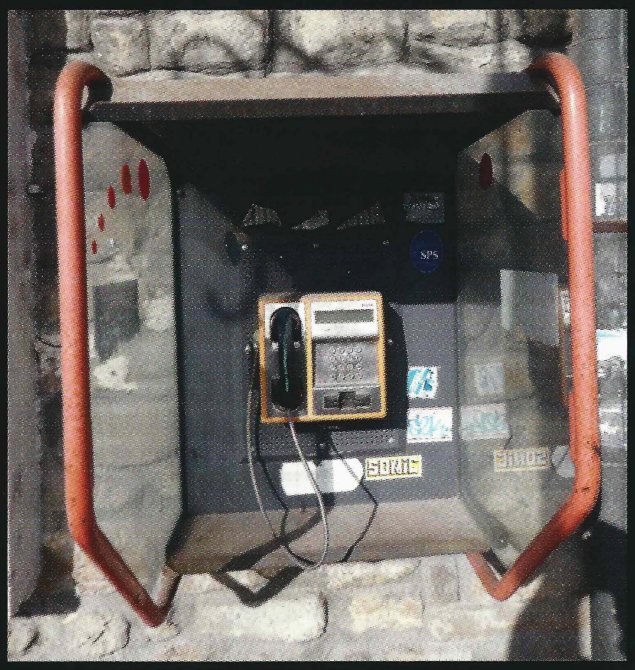
All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

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

International Payphones

Oman. Found somewhere in the maze of the Souq Muttrah marketplace in Muscat. This model can be found throughout the city.

Photo by Sam Pursglove



Bulgaria. This payphone, seen in Veliko Tarnovo, doesn't know how lucky it is. That amount of protection for such a tiny phone is unheard of in most parts.

Photo by Brian Collins

Spain. This is off the mainland a bit. Actually discovered in Las Palmas on Gran Canaria in the Canary Islands, this phone seems to have withstood lots of wear and tear. Run by Telefónica.

Photo by Oscar Sandström

Portugal. Again, not actually on the mainland. This one was found in Furnas in the municipality of Povoação on the island of São Miguel in the Azores. It also wins the award for the loneliest looking phone in this issue.

Photo by Kevin Costain

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

Here's a frame from the 2000 movie Romeo Must Die (spotted by **The Guy That Watches Bad Early 00s Films**) where protagonist Han Sing (played by Jet Li) is breaking into our apartment with a damn drill. Please. He couldn't even bring a lockpick set? In all likelihood, the reference was intentional since bypassing security is kinda our thing.

Who isn't enthusiastic about the Domain Name System? We certainly are and so is whoever painted this in the Sachsenhausen neighborhood of Frankfurt, Germany. Thanks to **Sam Pursglove** for discovering this. And if you search online with the above info, you'll find a whole bunch more tags from this artist.

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.