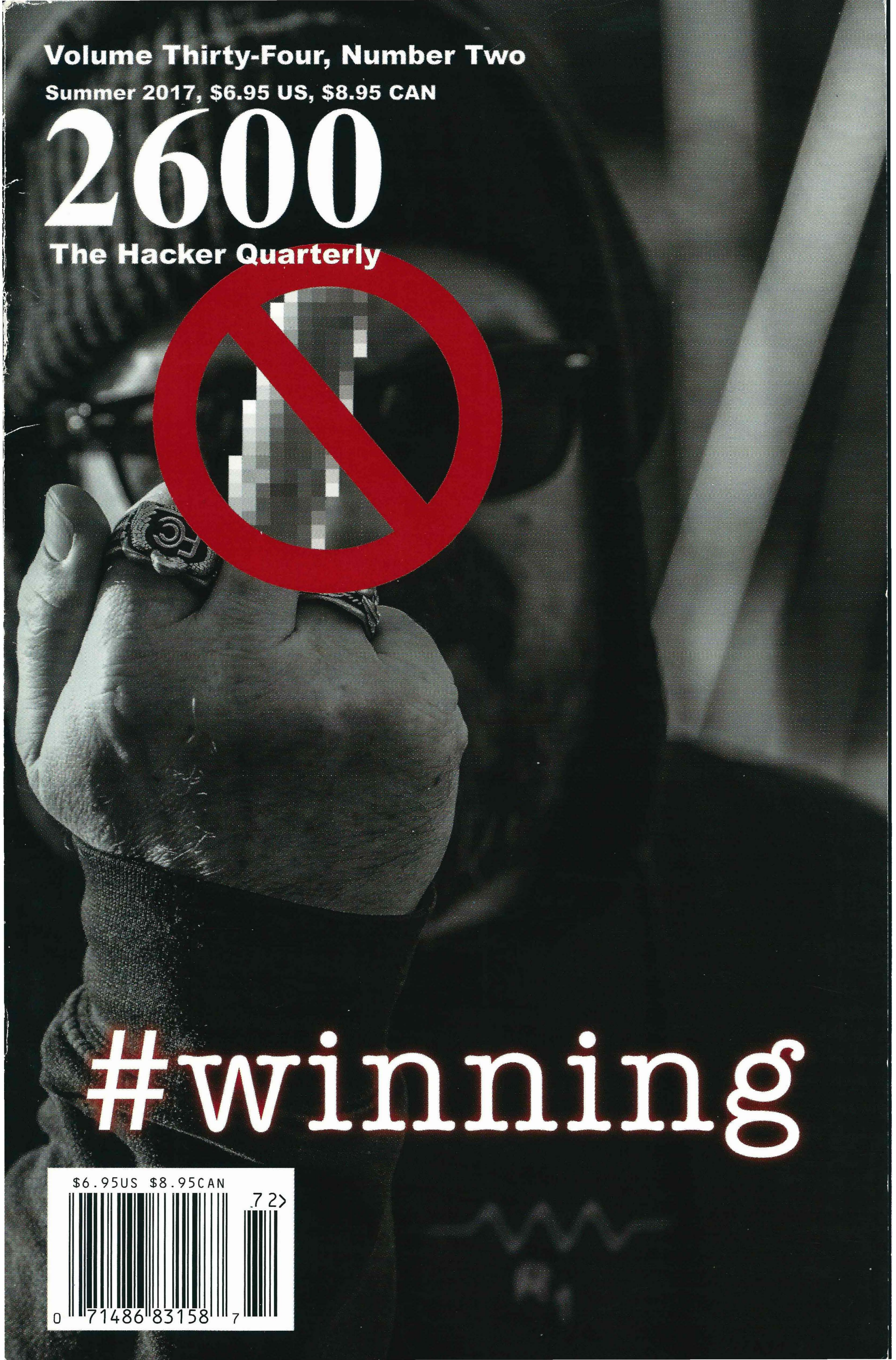
Volume Thirty-Four, Number Two

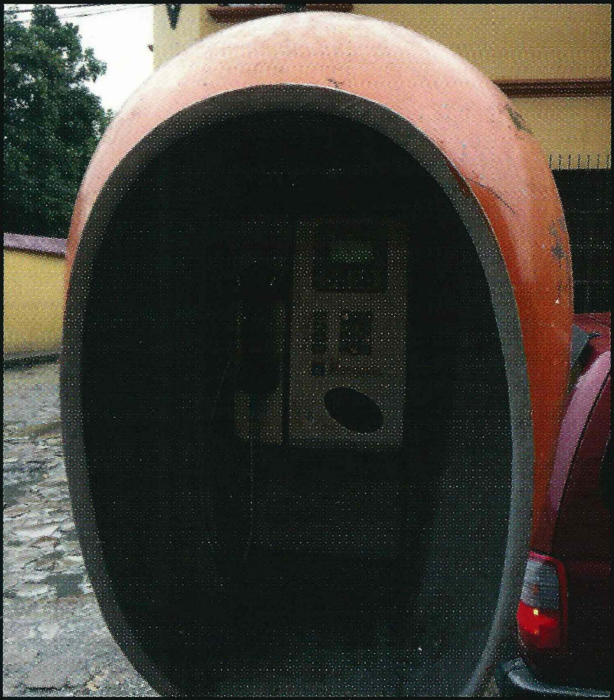
Summer 2017, $6.95 US, $8.95 CAN

2600

The Hacker Quarterly

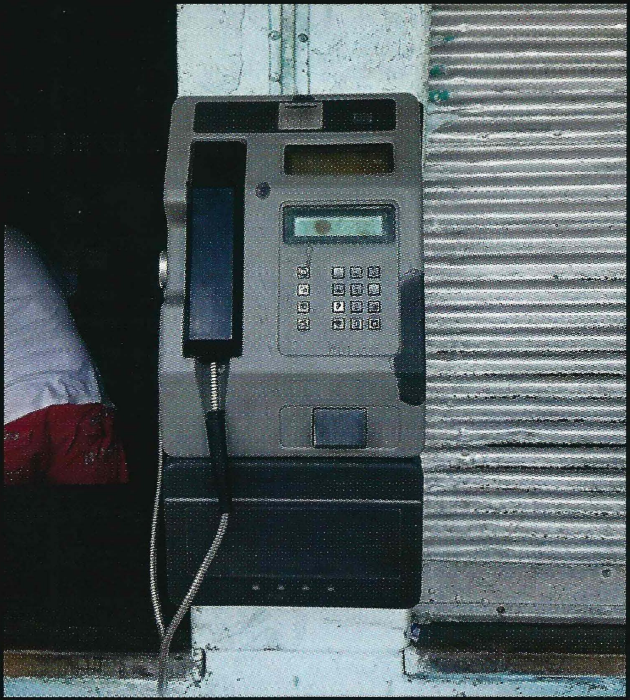


Payphones from Around the World



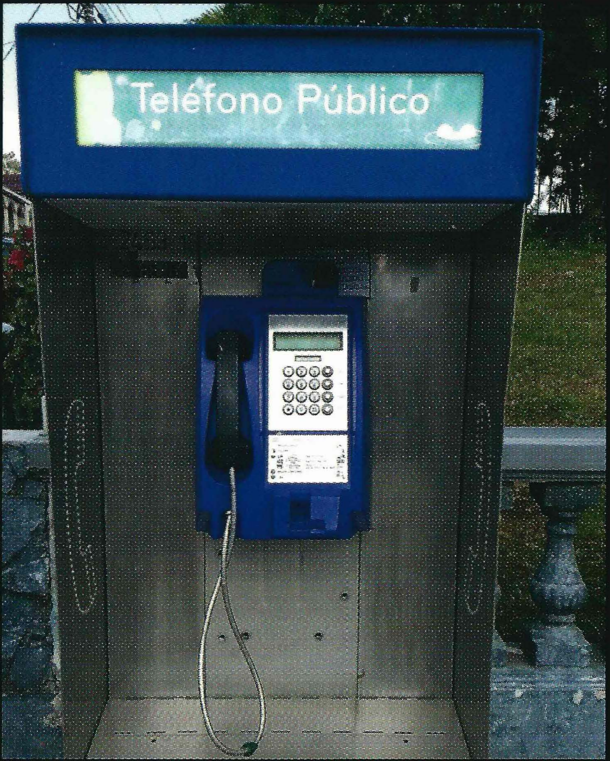
Honduras. This well-protected and stylish model is a government-owned Hondutel phone that was spotted in Santa Rosa de Copan.

Photo by Edwin



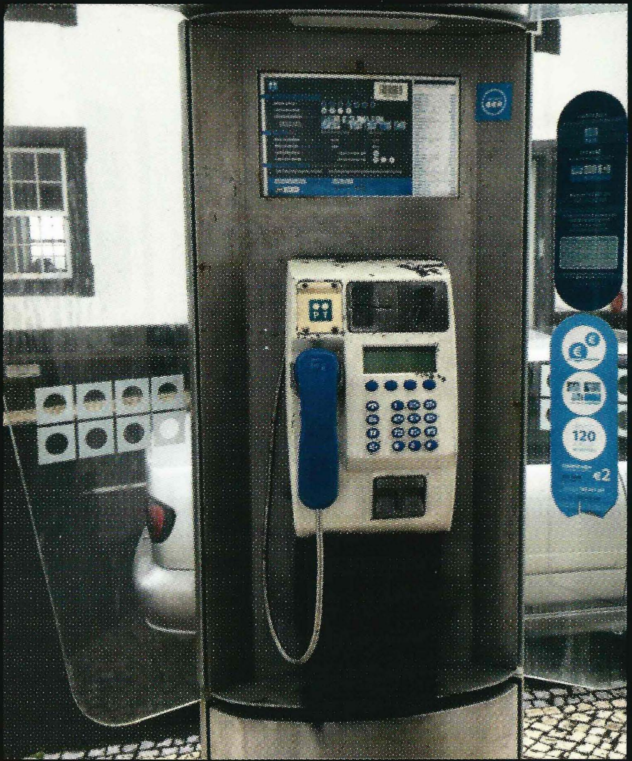
Cuba. This rather nondescript model was attached to the outside of a building about a block from Ernest Hemingway's old home in Havana.

Photo by Bruce Robin



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

Photo by Babu Mengelepouti



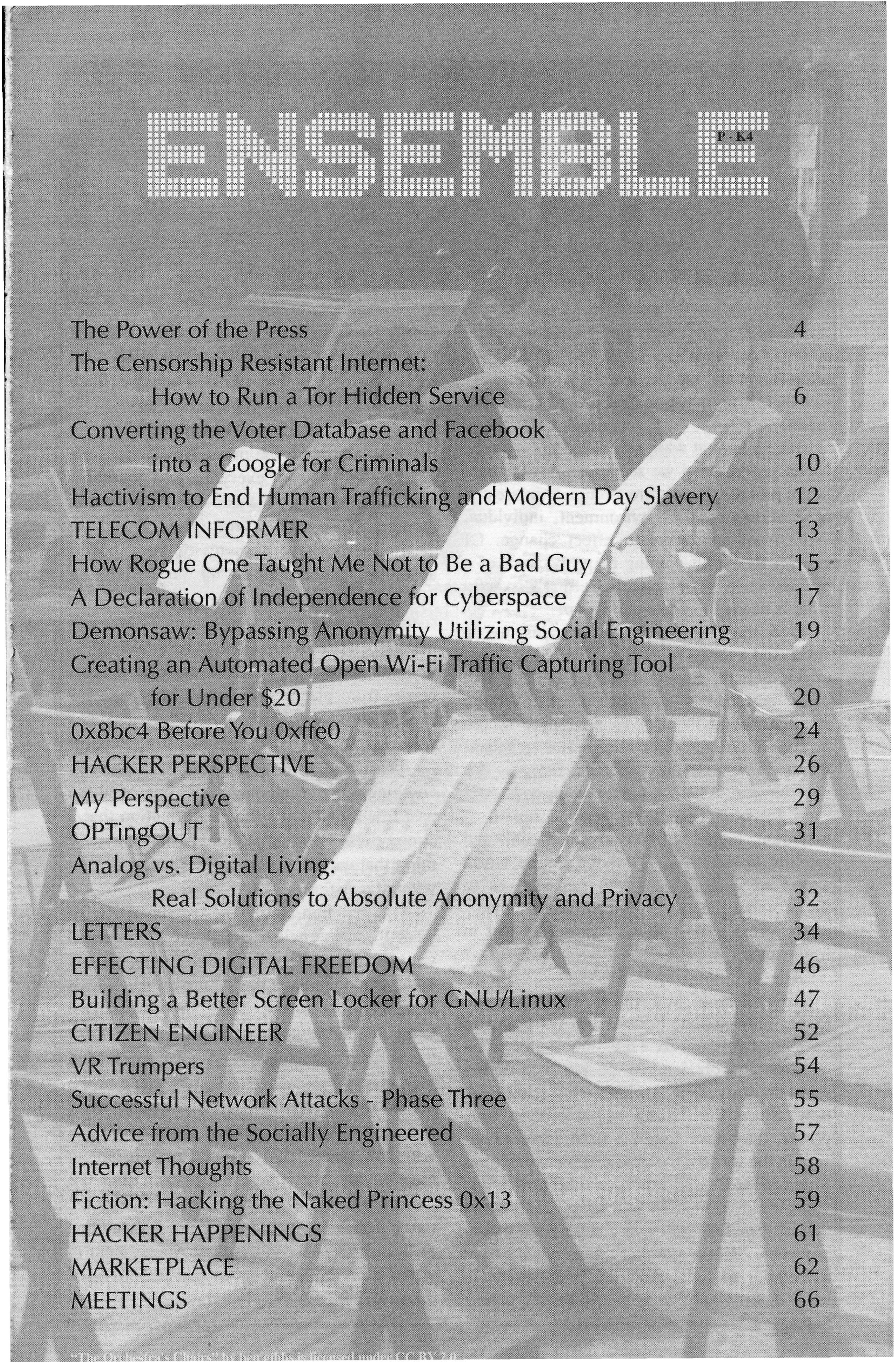
Portugal. Found standing all alone on a street near the pier in Calheta, São Jorge, Azores.

Photo by Anthony Cunha

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 (Do not send us links as photos must be previously unpublished.)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

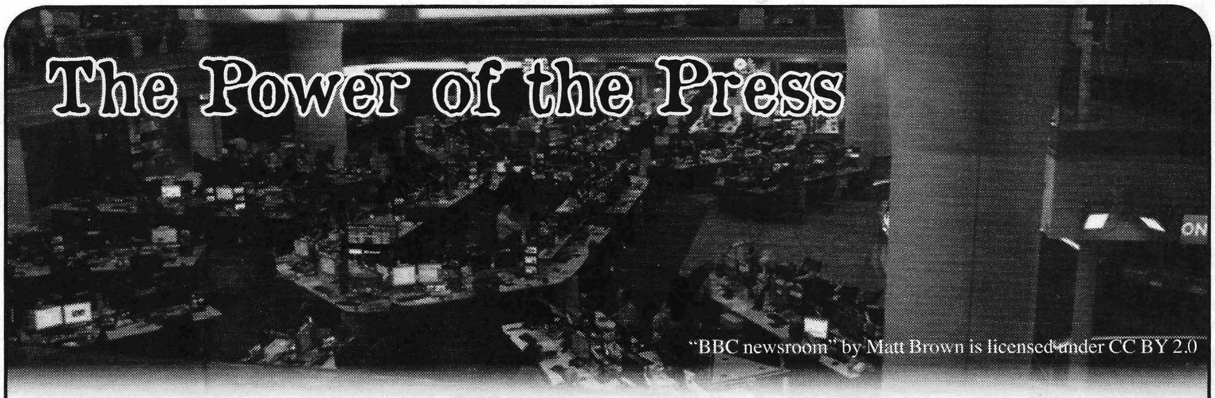
ENSEMBLE

P - K4



"The Orchestra's Chairs" by ben gibbs is licensed under CC BY 2.0

The Power of the Press



"BBC newsroom" by Matt Brown is licensed under CC BY 2.0

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

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

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

Almost.

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

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

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

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

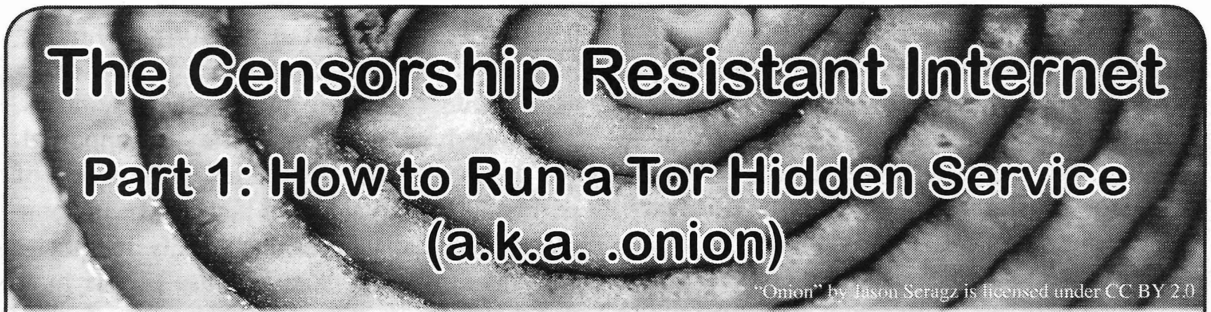
But while we're pointing out the importance and value of traditional media outlets, we don't want it to appear as if we're not also embracing the new technologies. These have, indeed, changed the playing field, just not in the ways that many are trying to sell. For far too long, journalism has been out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

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

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

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

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



The Censorship Resistant Internet

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

"Onion" by Jason Scragz is licensed under CC BY 2.0

by p4bl0
2.6k@uzy.me

0x0 - Introduction

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

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

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

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

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

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

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

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

0x1 - Where to Run a Hidden Service?

I make the assumption that the hidden service that we want to build is something like a small static website, so we do not need a lot of resources to run it, but it is better if it is always online. This is the perfect use for a low end VPS. It is not difficult to find very cheap VPS, something like $10 per year, if you are not too picky. Those are generally not to be trusted as your main server if you want to self-host your email or run your IRC client, for instance, but they are perfect for use as MX backup or to host a small hidden service.

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

0x2 - Installations

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

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

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

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

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

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

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

That's it.

0x3 - Setting Up Your Hidden Service

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

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

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

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

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

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

The next two lines tell the Tor daemon to listen on port 80 for this service and to forward the connection to port 8080 on localhost (a web server), and to do the same for port 22 (an SSH server). This will actually work with any kind of TCP services: web and SSH as shown above, but also SMTP, IMAP, IRC, XMPP, etc.

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

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

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

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

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

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

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

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

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

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

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

0x4 - Accessing Your Hidden Service

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

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

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

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

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

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

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

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

0x5 - Customize Your .onion Name

It is possible to customize up to some point your .onion name. There is a tool called Shallot[6] which simply does the brute force for you. There is no better way than brute force, otherwise it would mean that it is possible to derive the private key from the public key and that would be a *huge* security problem.

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

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

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

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

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

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

0x6 - The Setup for My Website

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

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

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

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

0x7 - Conclusions

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

0x8 - References

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

Converting the Voter Database and Facebook into a Google for Criminals

by Anthony Russell
Twitter: @DotNetRussell

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

Summary

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

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

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

How I Found This

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

Getting Your Seed Data

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

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

It can be found here:

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

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

Getting Information out of Facebook

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

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

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

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

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

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

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

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

Get name from profile page

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

Get profile photo from profile page

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

Get intro from profile page

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

Get details from intro block

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

Get links from details

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

Get text from details

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

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

Generating the Confidence Scores

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

Scoring the Name

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

Scoring the text

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

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

DANIEL <redacted>

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

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

Why Is This a Giant Problem?

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

Profiling

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

Creating spear phishing campaigns

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

Create wordlists for password cracking

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

How Can This Be Fixed?

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

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

HACTIVISM TO END HUMAN TRAFFICKING AND MODERN DAY SLAVERY

by Dr. G

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

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

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

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

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

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

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

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

References

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

TELECOM INFORMER

by The Prophet

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

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

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

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

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

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

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

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

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

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

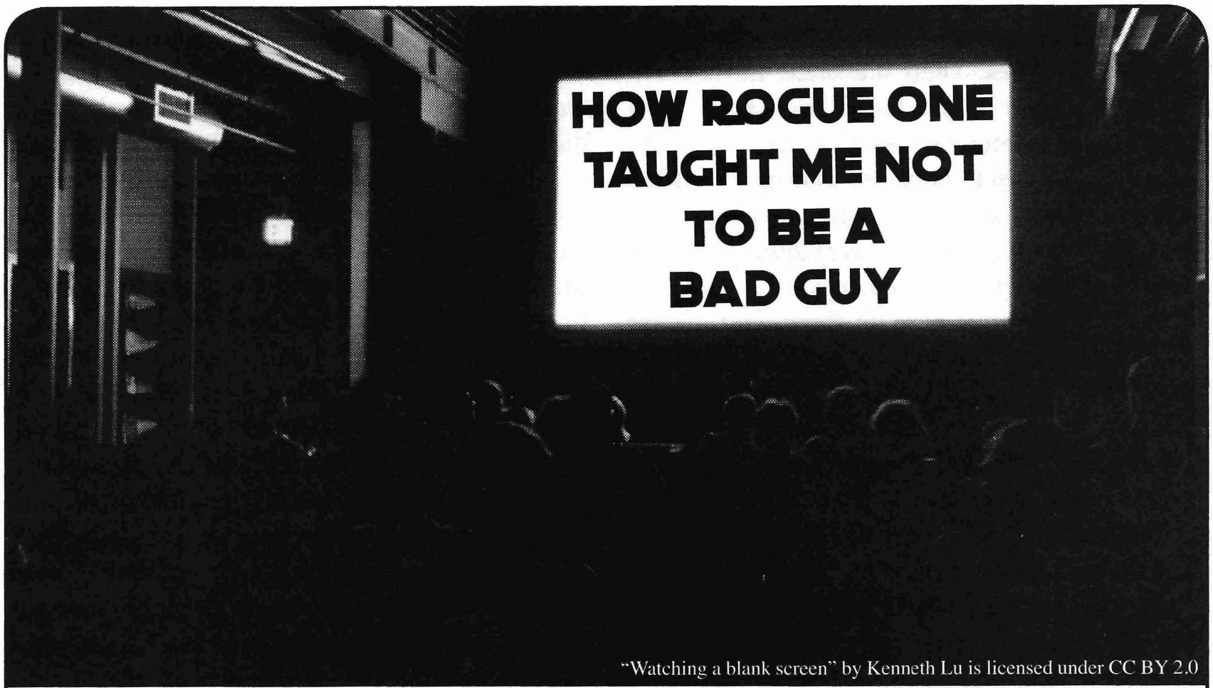
References

`http://www.taipeitimes.com/News`
`➥/editorials/archives/2010/10/05/2`
`➥003484569/1` - history of Taiwan country code

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

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

HOW ROGUE ONE TAUGHT ME NOT TO BE A BAD GUY



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

by Jameson Hampton

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

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

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

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

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

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

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

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

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

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

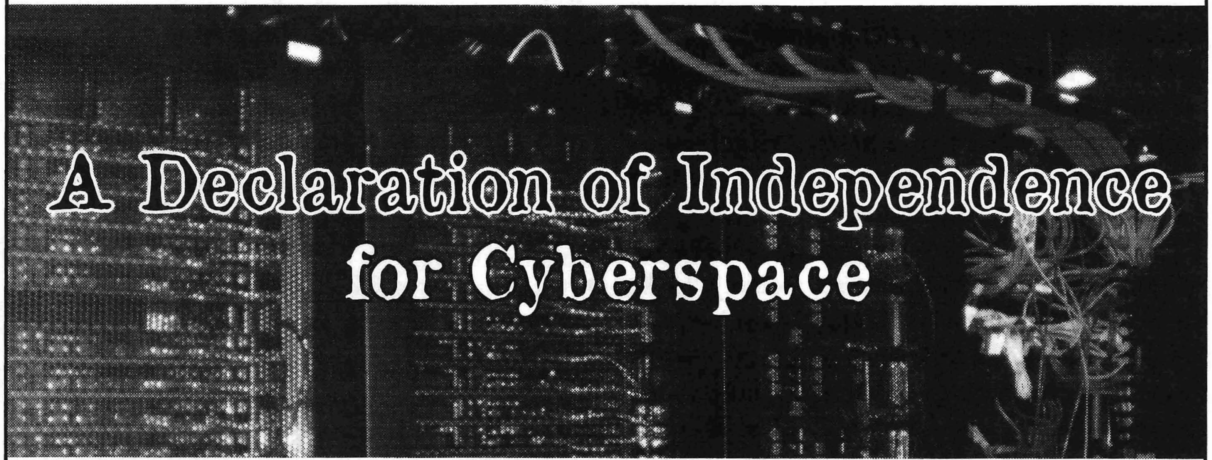
And then a *Star Wars* novel literally *tricked* me into working on the *Death Star project* and I realized that I had to do better than that if I didn't want to accidentally end up on the road to being a Bad Guy. I thought I was "safe" from doing evil because it would be obvious to me what evil looked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

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

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

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

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



A Declaration of Independence for Cyberspace

by Daelphinux

Section I: Definition of Terms

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

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

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

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

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

Section II: Declaration

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DEMONSAW: BYPASSING ANONYMITY UTILIZING SOCIAL ENGINEERING

by Hristo I. Gueorguiev
hristogueorguiev.com

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

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

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

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

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

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

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

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

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

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

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

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

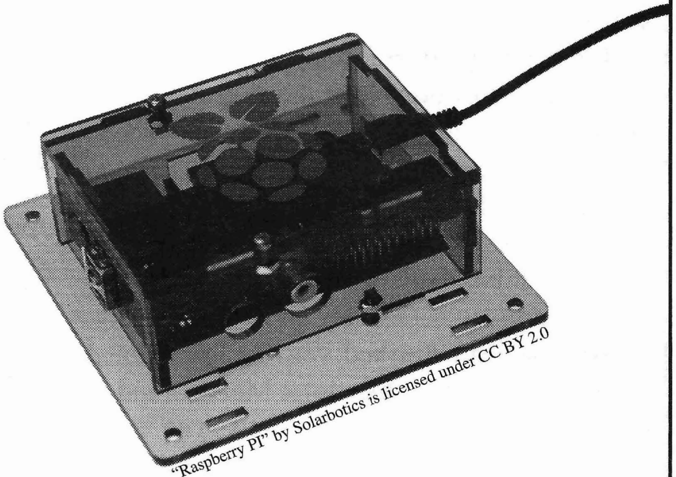
Of course, a driven attacker can even create multiple aliases and pretend to be multiple people to make more convincing conversations. Since anonymity is a built-in part of the network, there isn't a way to see if multiple aliases are actually the same person (well, other than the one discussed here),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

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

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

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

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



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

by Br@d

The Intro

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

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

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

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

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

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

The Disclaimer

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

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

The Pi

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

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

The NIC

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

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

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

The Battery

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

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

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

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

The Prerequisites

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

The Code

```
#!/bin/bash
# references the interface
wlaninterface=wlan0
# add the mon to the inferface name for use
with airmon-ng and airodump-ng
m=mon
i=$wlaninterface$m
# sets the base file name for the wireless survey
recon=/DaCaps/scouted
# sets the file name for the pcap file to write to
pcapfile=/DaCaps/DaCapFile
```

```
# sets the length of time to run the survey for - in seconds
recontime=120s
# sets the length of time to run the packet capture for - in seconds
capturetime=3600s
# general house cleaning to remove previous captures
rm $recon*.csv &> /dev/null
rm $pcapfile*.cap &> /dev/null
# setting wlan0 into monitor mode
airmon-ng check kill &
airmon-ng start $wlaninterface &
# running the wireless survey for the defined
amount of time then stops the process
airodump-ng -w $recon --output-format csv $i &> /dev/null &
sleep $recontime
kill $!
# finds the open Wi-Fi network with the most active
traffic and gets the channel number
channel=$(grep -a ‘OPN’ $recon*.csv | sort
-nrk11 | tail -1 | awk ‘{print $6}’)
# removes the comma from the output of the previous line
ch=${channel::-1}
#running the packet capture for the defined
amount of time then stops the process
airodump-ng --encrypt OPN --output-format pcap
--channel $ch -w $pcapfile $i &> /dev/null &
sleep $capturetime
kill $!
# our work here is done, time to take a nap
Shutdown -P now
```

The Automation

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

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

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

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

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

0x8bc4 Before You 0xffe0

by XlogicX

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

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

Back to Assembly

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

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

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

Machine Code

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

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

Micro Code

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

I digress. A simplified version of what the microcode for AAD is doing is: AL = AL +

(AH * base). This math assumes these values are hex, not decimal. AX is two bytes made up of AH and AL and the base is that machine code byte you supply after the D5. So to review our first example of "base 10" converting 1337: If we put 1337 into AX, then AH is 13 and AL is 37. To work the formula; 13 * 0A (base) is BE. BE + 37 is F5. At this layer of abstraction, the instruction worked as intended.

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

Exploitation

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

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

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

Summary

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

Resources/References/Filez

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

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

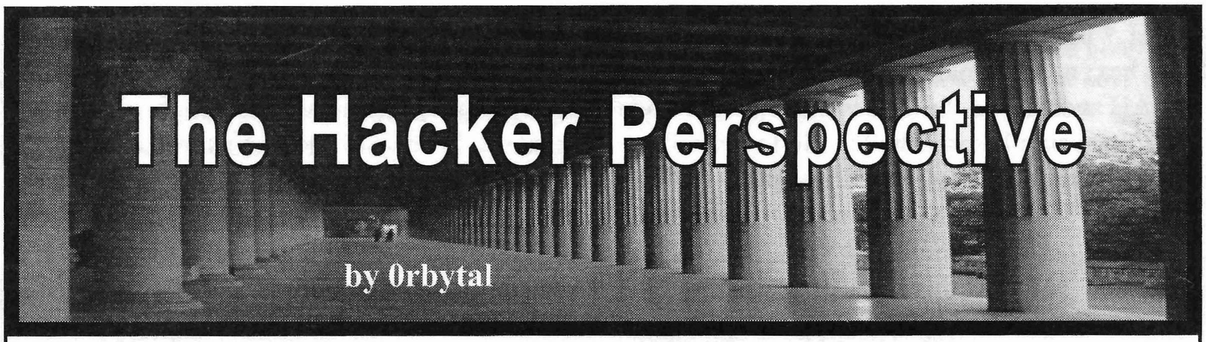
Intel Manual: `http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-manual-325462.pdf`

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

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

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

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



The Hacker Perspective

by 0rbytal

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Stay curious - and Hack *All* the Things!

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

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

MY PERSPECTIVE

by Buckminster Emptier

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

OPTingOUT

by Kernal Seiden

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

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

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

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

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

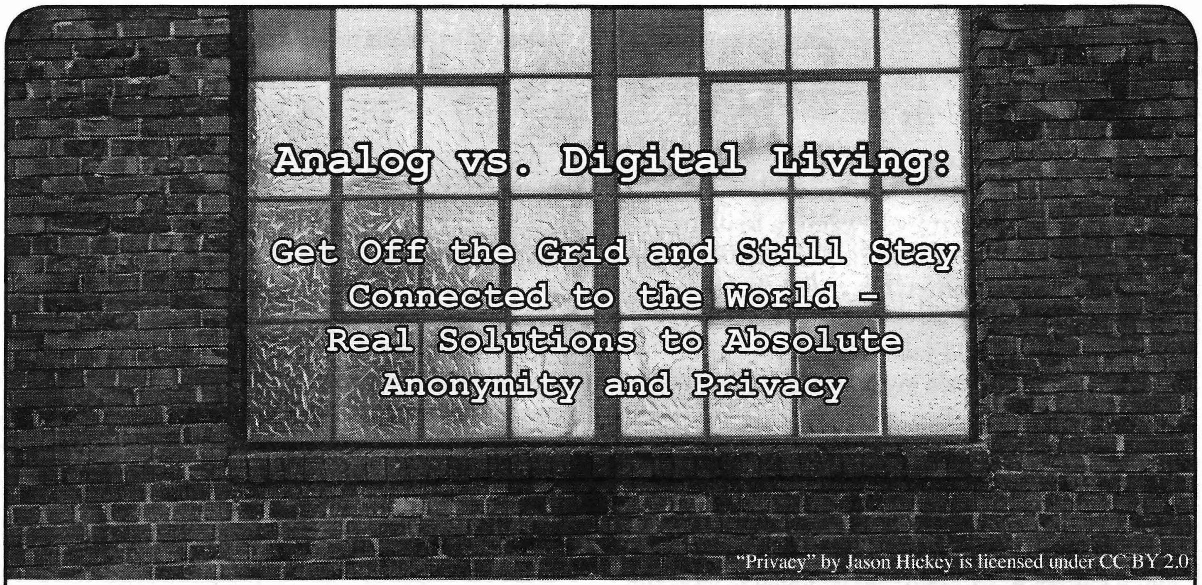
About a month ago, the frustration finally got to me, and I decided to tackle this problem once and for all. "There must be a way," I told myself. "There must be a way to actually 'delete' my account." So I dug, I clicked on every setting option on my Facebook app. Found nothing. I deleted the app and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

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

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

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

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



Analog vs. Digital Living:

Get Off the Grid and Still Stay Connected to the World - Real Solutions to Absolute Anonymity and Privacy

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

by DocSlow

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

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

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

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

Basic Anonymity and Privacy

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

Real World Security

Today's idea of computer security is but a farcical mess. Everyone is told that they can be secure if they only add on several prophylactic applications designed to protect the flawed operating systems they are so beholden to - mainly because they have been conditioned to believe that these operating systems are their only choice. These operating systems are continuously vulnerable because of their inherently flawed architecture - and can never be protected simply by adding the defensive sheaths of third-party applications.

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

Operating System and Hardware

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

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

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

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

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

Installing and Booting the Tails OS on the Chromebook

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

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

Conclusion

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

CHORUS CHORUS

Stickers

Dear *2600*:

People were asking for canvas bags and stickers on Twitter. You said you'd need some sticker designs so I made some. I DMed them to you on Twitter but figured I'd email you here. Hope you don't mind.

Hope you can use them, let me know if you do.

stAtiC

We appreciate the effort, but what you sent us was just our own logo from our website with "The Hacker Quarterly" written below it. That's a design idea we've already had. What we're looking for is something more new and unique.

Dear *2600*:

I am writing to different organizations and companies asking for free stickers. I started following *2600* about six or so years ago back when I came across the movie *Operation: Takedown*. I decided to really look into Mr. Mitnick and what really happened because I know of the way facts get distorted in "Based on Life" movies. I also found *Freedom Takedown* and watched it all for research. I really like what y'all have done for the hacker community and the information that y'all provide.

Back to the reason for this email. Like the subject says, I have a personal project that I started a week or so ago and I am emailing or using on site messages to different companies and organizations to ask for free stickers. I want to cover my laptop with the stickers I get and make a nice free sticker bomb type cover. I hope that y'all agree that this is a worthy project and agree to send me something that I can use.

Joe

How could we not agree that collecting a bunch of free stickers for yourself is a worthy project? But, as evidenced in the letter prior to yours, the creative forces haven't quite gotten to the point of producing something yet. We'll be sure to print an update when that happens.

Incidentally, our film was called Freedom Downtime. We've never seen it morphed into the title of the film we were opposing before. That's a little unsettling.

And while we're at it, Operation Takedown was the title of Takedown only in Sweden. Oddly, though Takedown was supposed to be the title, when it was finally released in the States years later, it was known as Trackdown. And for those who are really interested, it was first released in France under the title of Cybertr@que. And that's about all of the trivia on that subject we have.

Corporate Culture

Dear *2600*:

I'm Megan. I've been covering about emerging tech and latest technologies. Some of my works have been quoted and featured in *Entrepreneur, Inc, Huffington Post*. I'm currently looking to expand my writing portfolio and was hoping to write for *2600: The Hacker Quarterly*.

Would you be the best person to pitch ideas to?

Megan

Why do we have this unsettling feeling that our name was simply inserted into some mass mailing and that you have no idea what we're really all about? Because if you did, you wouldn't be surprised at seeing your letter printed here along with our skepticism. For one thing, the email address you sent to isn't a "person" and we generally don't entertain pitches, product placement, or corporate speak. With that out of the way, we look forward to seeing what you have to share with the hacker community.

Dear *2600*:

I'm Ellie Martin, business and tech writer with focus on emerging technology, marketing, and science. Some of my works appeared on *Business Insider, The Next Web, Computer World,* and a few other publications.

I'd love to explore the idea of contributing articles for *2600: The Hacker Quarterly* readers and I was hoping to run by you a few topic ideas. Would you be the best person to pitch those ideas to?

Ellie

Well, now isn't this a coincidence? You used almost exactly the same phrasing as the previous letter writer! Do you know each other? Perhaps you could combine forces and write a really super article? We'd love to see what you come up with.

Dear *2600*:

My name is Praful Mathur, roboticist and cofounder of Shotput, an advanced 3rd party logistics company poised to give Amazon and FedEx a run for their money. Backed by YCombinator and Justin Kan, Shotput uses robots and AI to address the fulfillment needs of fast-growing e-commerce companies.

Here at Shotput, we install robots in shipping containers to create automated micro-warehouses. Using AI, Shotput determines optimal locations throughout the U.S. to minimize shipping time and maximize consumer reach. Here's what sets our tech apart: [redacted]

I would love to tell Shotput's story in *2600: The Hacker Quarterly* and I think your audience would love to learn about our tech too!

Thanks!

Praful Mathur
Shotput Co-Founder and CEO

OK. First off, this actually does sound like something that could be of interest to our readers. But this appears to be yet another corporate PR piece and that instantly turns us off to the idea. We had to take out all of the enthusiastic bluster about how your tech is a true game changer, milestone, etc. because it was being flagged as spam in our desktop publisher (a feature we didn't even know it had). So, if in fact this is a person mired in a corporate pitch, we hope you can extricate yourself and write about the actual tech, but not in a tone that sounds like a marketing ploy. There are truly some amazing things going on in this field, but we're interested primarily in the technologies, not the companies. If you can work within those parameters, then by all means write something.

Further Info

Dear *2600*:

In a recent issue, an article was posted about booting a Mac OS X computer into Single User Mode by holding the command key accompanied by the S key. This is correct, however it can be a little more nuanced with more recent operating systems. First of all, booting into Single User Mode will require an administrator password unless Firmware Password Requirement is turned off in Recovery Mode. Recovery can be booted into by holding the command key and the R key. While in Recovery, it is a good idea to decrypt the computer's files using FileVault (or lack thereof). Booting back into Single User, run the "fscky -fy" command. This will take some time. Follow up with "mount -uw". You'll have to launch the Daemons, using "launchctl load /System/Library/LaunchDaemons/com.apple.opendirectoryd.plist". After this, "passwd" commands will go through with no trouble. Thank you for your time, I hope this helps someone!

Akalabeth

We have no doubt it will.

Dear *2600*:

In Dr. G's article on U.K. surveillance (*2600,* Spring 2017), a minor blind spot was demonstrated. It has been years, if not decades, since PGP was a pain in the ass to configure, or considered marginal technology.

Here's a method that I like to push on people who are reluctant to take all the appropriate steps to secure their info, but want the result with minimal effort.

Horde webmail comes out of the box with many hosting providers, including HostGator, with PGP support built in. All you need to do is associate an address book, create a key for yourself, import keys from others, and check the sign/encrypt box. Double-advantage: Your email is not stored on your local machine, and what *is* stored is encrypted. Your private key is stored on the server, but your passphrase is not. I know that rubs some people the wrong way, but with a strong enough passphrase, it should be a fair tradeoff.

Also, mail clients for Android (such as R2Mail2) support PGP as well. So if you *must* have your encrypted emails on your phone, you're good to go.

bobgerman

Thanks for this most helpful suggestion. It's exactly the kind of thing that will get more people using encryption, even if it's not 100 percent the way others would go about it. The key is to get people realizing that encryption is beneficial and normal and, to get them there, we need to make it as easy and transparent as possible.

Dear *2600*:

Hi, I left a message regarding Anycon.info. This is the first conference of its kind in upstate NY featuring a very unique CTF, Hardware Hacking Village, and Lock Picking Village. This will be June 16-18 this year. Would love to get your feedback.

Laurie

We would have loved to have helped publicize it but, as you can see, it's now past June. For future conferences (and for anyone else interested), make sure you let us know at least a month before our issues hit the stands (which is generally in early January, April, July, and October).

Dear *2600*:

While on the topic of book recommendations, I would highly recommend the book *Weapons of Math Destruction* by Cathy O'Neil (she blogs at mathbabe.org). When taking classes on big data during my (ongoing) graduate studies, the classes were required to talk about ethics, but the CS faculty's idea of ethics didn't seem to extend beyond issues related to privacy. Sure, privacy is important, but ethical issues with algorithms and big data go beyond privacy. We have data-driven black boxes and poorly justified mathematical formulas trained on data points that are human beings and then making decisions affecting the lives of said human beings.

Here's a brief summary of the issue this presents: Algorithms lead to people getting custom content, either paid or unpaid, and it's difficult to know, from a "global" perspective, how these decisions were made. This leads to vulnerable people getting ads from the University of Phoenix preying on their insecurity and ultimately saddling them with enormous loans in exchange for shit degrees (did you know they give PhDs? I really want to meet someone who got a PhD from the University of Phoenix; that must be a special kind of idiot). Then you have people's world view being shaped by the content fed to them by an algorithm, which could be all crap, and politicians can target advertising so people see lies they in particular are likely to believe (this was a factor in the last election).

Then there are formulas that cut people off from credit or discriminate unjustly. There are arbitrary formulas that deny people jobs or get them fired because they don't meet some arbitrary standard. I think I personally have been a victim of this: when I graduated from high school in 2010, I was desperate for a job (my first job). I applied to be a cashier at Sears, with the local store having a ridiculous number of open cash registers, and I was directed to a machine that, after a handful of questions, rejected me for mysterious reasons. I never got a chance with a human being! (I'm now a PhD student in mathematics in a highly ranked department studying from leaders in their fields, and I'm told I'm one of the best grad students there, so I think I was capable of running a fucking cash register.)

I could go on, but no one wants to read that (unless you'd like an article summary; I could do that). I read this book in a day, and I think hackers would love it. It's easy to read, but all the stuff in it should convince people this is an area that needs more attention.

On a side note, I read 33:4 and 34:1 and I enjoyed them, so I'll be subscribing now. You can also probably expect an article from me in not too long, too. Good stuff!

NTGuardian

Thanks for that enlightened outlook and the well-deserved critique. It's probably a good thing that you were spared from Sears. We look forward to your future submissions.

Dear *2600*:

Staying on the topic of hackerspaces from my last article, I will let you in on some information I've picked up during my time as a member of two different spaces. I'm a software guy by trade, but by being a member at a makerspace, I've accidentally learned some other things.

To me, the makerspaces have been invaluable as there is always some sort of semiformal class or lesson on various topics. Different spaces will have different rules on nonmembers using the tools and different payment setups; it's always good to check them out on a public night first. Our local makerspace has a daily public open house based around a learning theme. This ensures there's at least one member there that knows how to use the related tools to help everyone. Monday wood shop, Tuesday programming, and so on.

From building picture frames to furniture to mobile apps and desktop apps, the curious type willing to drop in on a public night or set up a tour with a member can learn almost accidentally. It's not just the tools and workspace that makes hackerspaces useful; it's also the sharing of the skills and knowledge of the community of members and visitors. It's great to be able to bounce ideas off of people and get help for the parts of my projects I'm not very knowledgeable about. Group projects at makerspaces are one of the most fun ways to learn.

Recently, we built our own Hobby-Vac vacuum former to use for things from making chocolate molds to costume parts for cosplayers. There was lots to learn on this project from woodworking the dovetails on the main body to drilling for the metal platen to the plumbing of the air hoses and valves for the vacuum tank and pump to the electrical wiring of the switches for the heater coils and the pump including a safety fuse. The experience let me gain knowledge in areas I didn't even know I would learn about.

If you've ever wanted to learn any topic from metalworking, woodworking, electronics, 3D printing, laser cutting, robotics, programming, or even network security, make sure to find your local hackerspace and take a tour. Learning together is the name of the game with hackerspaces. Go find your local space right now! Note: Usually a quick Google search for "makerspace [your city]" or "hackerspace [your city]" will give you a good start. You can also check out the hackerspaces.org website for help finding your local space. And remember, if you don't have a space close enough, don't be discouraged - create a meetup.com group and you can start one up.

RAMGarden

From this perspective, hackerspaces and makerspaces seem fairly interchangeable. There are, however, differences with every space: some are open to everyone, some are semi-private, some are very limited. But one thing that seems to be the same everywhere is the notion that we're much better off having them around than we were before.

Dear *2600*:

I am writing this article exclusively for *2600* in a series of posts about general iPhone security for the consumer. In this article I will cover common iPhone PIN cracking techniques and some fun exploits with Arduino/Adafruit that will make pentesting your iPhone tons of fun if you have some extra cash to burn on a proof of concept.

The main device used in iPhone PIN cracking is the pre-assembled official 3D printer from Arduino. I am most familiar with this brand which is why I chose it and it is relatively affordable for a 3D printer, but almost any 3D printer can be programmed to hold a stylus and enumerate PIN combinations until the phone is unlocked. There are some videos on YouTube of a Garmin device being cracked with a 3D printer array, so the concept, although very clever, is not a new approach to testing iPhone security. Having a 3D printer around adds the extra fun factor to it because there are a ton of things you can do with a 3D printer besides pop iPhone PINs, like make parts, toys, or functional devices out of it.

The device is $779 from the Arduino USA online store and the Arduino Materia 101 comes assembled or in a kit form.

The second fun thing to do to test your iPhone is to bring online as many Wi-Fi or Bluetooth nodes as you can until you experience a denial of service. This is commonly found in large gatherings where there are a lot of mobile phone radios and Bluetooth radios turned on all trying to communicate with one another, which results in a denial of service. Well, the power of a roomful of people's Bluetooth devices can be easily simulated with an array of 100 or so Bluefruit line devices from Arduino's online store. They have many different form factors for programmable Bluetooth/IoT devices which range from around $19.95 to $29.95 per Bluetooth module/kit. This is a great addition to your Wi-Fi network survey as Bluetooth PAN network surveys are often overlooked.

Matthew Sacks

As this was so short, we thought it would be more appropriate as a letter. We'll certainly consider running more in-depth pieces on this and other subjects in the future. Thanks for writing!

Dear *2600*:

Yes, that is how *2600* is displayed (34:1, page 38) whenever I go to the Houston Micro Center. I know of at least one company that trolls for new employees there. He hangs out in the specific aisle of interest looking for potential candidates. Not a bad way to find a new nerd/geek hired hand.

B

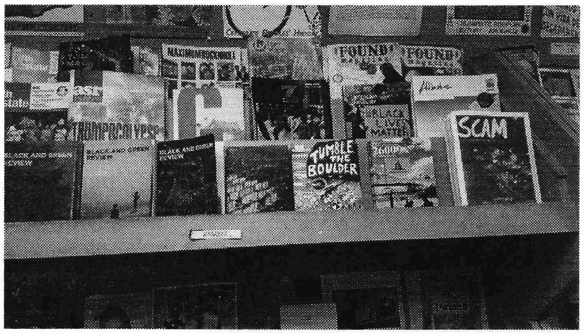
Sounds a little creepy and strangely similar to how migrant workers are found for cheap labor outside Home Depots. Hopefully, we won't see people taken advantage of here.

Dear *2600*:

The Wooden Shoe is a fun book store here in Philadelphia. I wanted to share a photo of them stocking the magazine at this anarchist bookstore collective of their top-shelf placement. Hope all goes well. A random HOPE name idea is "HOPE yet." I cannot remember if I pitched that one. Granted, it's a whimsically simple name.

Pic0o

It's always heartening to see our magazine in the company of all kinds of other interesting publications. We'd love to see additional pictures of it being treated right in stores.



Concerns

Dear *2600*:

I am writing to you about the threat and possible backlash or strikes that might be delivered by the Trump administration. I am here to say never fear the two party oligarch rulership. The two party oligarchy is obviously and laughably facilitated by the owners (one percent). The reason I say never fear is that the owners and oligarchs forgot one thing. They need us, the people, to get anything from agriculture, construction and yes, computer programming to get their objectives completed. So, without us, their lofty positions and titles mean nothing. I'm glad to see that *2600* took the more logical route letting the readers know that "We are the People." I'm also writing to confirm that I will stand up with the people of my country and globally if necessary... there are actually bigger issues to be concerned with than Donald Trump and the size of his penis. For instance, did you know that CERN has an insidious objective with the Large Hadron Collider? They want to create a mini black hole to send a graviton through.... wow, yes really, it's true. Google it, it's on their web page. Black holes start off small and grow. What makes these scientists think that they can control a black hole? And just like you said in the Spring letters column: "After all, it's in the darkest hours when a bright light makes the most difference." Understand this, light cannot escape the power of a black hole. So to the readers, please don't be fooled by the brainwashing of Hollywood and politics. Look to real threats that could end our entire existence as we know it.

Tyson

We probably should have said "it's in the darkest hours when a bright light makes the most difference - unless you're sucked into a black hole in which case nothing at all will matter." Perhaps that suffix should just be assumed in the future so we don't have to append it to every point we make. Oddly enough, even after you told us of your concern of a black hole enveloping the entire planet, we still keep seeing Trump as a bigger threat. The scary thing is that he probably would take a good amount of pride in that.

Dear *2600*:

The Library of Central Bank of Bolivia, you not wish to receive reports or printed publications *2600 The Hacker Quarterly,* because it no longer has room for storage.

Please do not send printed publications, we are not interested.

We do not have physical space.

Kind regards

Sikorina Bustamante Paco
JEFE DEL DEPARTAMENTO DE BIBLIOTECA

OK, just settle down. We never sent you any issues in the first place so we don't know what *you're getting all upset about. It's hard to believe our digest-sized publication would cause you this much grief in the first place. Clearly, you guys aren't managing space very well. You've made us so curious that we feel compelled to visit and make some suggestions. Come to think of it, why does a bank even need a library? Isn't that what libraries are for?*

Dear *2600*:

First of all, thank you for printing my article! I have gained much more experience now, but I am still proud of my piece in 34:1!

So, now to the main point.

On page 41 of 34:1 (the letters section), I found a piece of paper with the following text on it inside:

www.mgtow.com, www.dontmarry.com, www.avoiceformen.com, www.leykis101.com, Nevercosign @ ok cupid, www.mensrights.com.

The text is exactly as printed, but in Times New Roman. I did not visit any of these sites, but they appear to be men's rights websites.

Was that supposed to be there? I got my copy of 34:1 at a Barnes and Noble near Atlanta, if that helps. I don't think it was supposed to be there, personally.

ckjbgames

Your thoughts are correct - we don't stick cryptic messages in our issues, other than the ones we print in our own pages. We have no clue what any of this is about, but if it was in only one copy, then it was likely a rather strange mistake somebody made. If the same message was stuck in multiple copies, the strangeness factor only increases. (Incidentally, sticking messages in issues is exactly how many local meetings help get the word out. We don't object to this method of reaching out as long as the issues aren't permanently altered in any way.)

Dear *2600*:

Just a year or two ago, you all claimed you were in financial straits thanks to a publisher. And yet, you are offering $10,000 for the current President's tax returns.

As you point out, it is *not* a requirement for a presidential candidate to divulge their taxes and, frankly, I don't remember who started that or when, but you indicated it has been done for decades. Frankly, unless you can document when and who, your claim is an exaggeration.

However, to qualify as President of the United States, it *is* required that the candidate be an American, born in the United States. When asked if he would run for President, Arnold Alois Schwarzenegger said he could not run, just for this very reason.

All of the Obama supporters poohooed questions about his qualification to be President based on birth right and he took over two years before producing a birth certificate in an attempt to dispel this controversy. So where do the liberals come off demanding documents that are not required?

Now don't tell me you might be concerned about executive manipulation of the IRS; I would trust the current administration more than the previous one.

Given your current stance, I plan to let my subscription run out without renewing. If you have $10,000 to throw around for Bull Shit, you don't need my subscription and, frankly, the magazine's content within the last year and a half has been pitiful.

DM

We fear your logic is becoming lost within your partisanship. Let's address your points in order. It was a distributor who caused us financial woes (again), not a publisher. We're the publisher, hence the publication. And yes, we've managed to recover. Thanks for noticing. But we're not simply throwing money around. First off, we're not spending a cent unless we get the returns and nobody who participates in our bounty will either. So right now, it's little more than wishful thinking on our part. You clearly think that's a bad thing and the only reason that springs to mind is that this is a candidate you support. You apparently have no issue demanding a birth certificate from the guy you don't like, a document that wasn't requested from anyone else. That contrived "controversy" was really hard not to see as blatantly racist. Tax returns, however, have been routinely divulged by presidents since the Nixon days. The documentation you want in order to back this up is right there. This is a fact, not an exaggeration. And, while we said up front that this has never been an actual requirement, why would you support changing this tradition at this particular moment in history when financial improprieties are very much being seen as a strong possibility? Trump demanded Obama's birth certificate even though that wasn't a requirement and Obama produced it to put the myths to rest. It's really strange that this desire to put another supposed myth to rest doesn't seem to exist amongst Trump supporters. In effect, that casts more suspicion on his finances than anything his critics are saying.

You're welcome to your opinions on our content, but we have never seen this level of enthusiasm from both readers and writers in the hacker community. Remaining in that environment, even if you disagree with some fundamental points, doesn't seem like such a bad idea. We make this same point to people who want to move out of the country because of what's been going on. When things get crazy, that's when your voice can make more of a difference than ever. Unless you're sucked into a black hole in which case nothing at all will matter.

Dear *2600*:

You have always been a beacon of hope in the dark. While being sure to issue disclaimers, you never actively betrayed your fellow man or worked to harm them. This is not so with your IRC network you publish in the back of the magazine.

One of your IRC admins has worked for the FBI in the past and is a federal agent. I urge you to stop allowing him to use *2600* and likeness. He has taken over your *2600* Facebook in a hostile manner. He operates with other known agents in the IRC community and Facebook community actively attacking these groups while running them. If new people come into your IRC, they are banned or treated as outsiders. It is a group now of regular people who see fit to only chat with those that they know. This has never been the *2600* mentality and meetups are always open to anyone. Even if federal agents were running *2600* meetings, they still operate in an open fashion and, if discovered that they were attacking the local community, they would be quickly outed.

I urge you, for the sake of community, to not publish this IRC network as affiliated with *2600* for the sake of people joining this network seeking like-minded individuals, and I urge you to take back the Facebook page or remove this person from control.

I regret that I will be pirating *2600* and not sending you a dime until I see this IRC page removed or his network disbanded. I will also be actively boycotting and distributing your content for free to anyone and everyone who wants it and urge them not to send you a dime until this matter is corrected.

Concerned lifelong *2600*'er

In your world, did you think that last paragraph was the thing that would convince us that you were on the right side? You had a bunch of us standing on our chairs, pumping our fists in the air, and saying "At last someone has the guts to speak the truth!" and then you went and threatened us and everyone sat back down and got back to work. (Actually, none of that happened, but you seriously need to learn how to effectively get people on your side or you'll simply wind up doing the work of the people you oppose.)

To address this issue, we have had people running IRC networks and Facebook pages in the past who have walked in different circles or have even done things that we found abhorrent. (We are unaware of any federal agents ever filling these roles.) But if they did the job and/or were the people who set the thing up in the first place, we didn't impose our opinions on that. However, if they did something that affected user privacy or started to work directly against us, we stepped in and corrected the course. In this particular case, the admin in question (we removed his name and handle as we don't want this to become about personalities and perpetual back and forths) has done nothing to adversely affect the operation of either the IRC network or whatever Facebook page we're talking about (we've honestly lost track since there are quite a few). We know personalities can often collide and when somebody has enforcement power, accusations of abuse are inevitable. We simply can't get involved each and every time this happens and, without specific and repeated examples of abuse, you haven't really given us anything to go on. One thing we've learned in our community is that we often work with people who have radically different perspectives, philosophies, backgrounds, and political ideologies, and that this is more an opportunity than a hindrance. We speak our minds in these pages quite often and, either people agree, debate us, or walk away. It's only the latter who lose because they've cut themselves off from any possibility of dialog and understanding. While this may not make you feel any better after having been kicked out of an IRC channel, it may help you to put all of this into perspective. IRC and Facebook aren't worth getting bent out of shape over.

If your answer to anyone you disagree with (or who doesn't do as you say) is to boycott and attack, that's something you really need to look at.

Meeting Updates

Dear *2600*:

There has been a misunderstanding about the *2600* meeting location in Chicago. There was another security meetup at the Space by Doejo location and a newcomer must have gotten confused. It's pivotal that we have it changed back by the next print.

I have lobbied to include your audience in our group and have the whole community engage together, but Doejo isn't having it. Apparently, they are having the sudden epiphany that "security" is corporate doublespeak for "hacking" and our group has been suspended from meeting there until further notice now, too. Perhaps one day hackers won't be such a feared or misunderstood community of people, but as long as the narrative invokes enough fear to convince people to surrender their privacy and liberty to overzealous authoritarian rulers, I don't see it happening anytime soon. At least not for four years.

Travis

This is extremely confusing. We don't know if you're speaking on behalf of our meeting or another. We don't know how or why a newcomer was confused, although we can certainly relate. And our listings for this meeting have been the same for well over a year, so we have no idea what you're saying we should change it back to. As far as we know, the Chicago meetings are taking place in the usual location. This kind of thing is why it's a great idea to have websites that can be updated if something changes.

Dear *2600*:

You hear from the Chicago people lately? Still listed, but all info I can find on the web seems pretty outdated.

Phil

We don't know where on the web you're looking as this meeting doesn't seem to have a website. That would certainly make things less confusing. Hopefully, this will be worked out soon.

Dear *2600*:

Last night was the largest gathering of *2600* readers ever held in Titusville, Florida. Three other *2600* readers showed up and, amazingly enough, all of us were ham radio operators. My brother from upstate New York was visiting me and also came by, but more out of curiosity, and was able to hold his own in conversation when technical audio subjects came up. Total attendance: five.

I would appreciate it if the Titusville listing included the Three Words for finding it, with notification to all meeting planners to send in updates to their listing with What Three Words locations included. Here's mine: Titusville: Bar IX, 317 S Washington Ave. followers.ambient.radio - W3W.co/followers.ambient.radio. And that's the news from Port Wobegon.

Richard Cheshire
Phreak & Hacker

Congrats on having decent attendance. And yes, a handful of people is a success if the company and conversation are pleasant. Some places will have many people, others far fewer. But the spirit is what counts and if you have that, you're doing great. We hope others who are trying to start meetings in various places see this as inspiration and don't give up if it takes time to find other kindred spirits in your area.

The what3words.com website has more info on how to define your specific location with three unique words. It's an intriguing concept, one we've used on a recent cover. Every three meter square has a unique three word geocoding address, even those in the middle of the ocean. It uses a database of around 40,000 English words and is also supposed to work in 25 languages total. One thing it can't do is distinguish differences in height, so if you're trying to define a unique address in a skyscraper, you'll have lots of company. If this way of defining locations becomes popular with other meetings, we'll start adding them to our listings.

Dear *2600*:

We had our April *2600* meeting recently in Edinburgh. A lot of folks showed up due to the BSides event that happened in Edinburgh on the same day. So this was basically a pub takeover and some.

Overall, we've been having good turnouts (about 15 folks) with a few new faces, which is great to see. What's so nice about these meetings is the blend of people with different backgrounds and interests. So hopefully the momentum will keep up. Good to see peeps from different backgrounds, from reconverted blackhats to newcomers.

Suffice to say we got way jolly. So all around a great night.

stmerry

Great to see this meeting taking off, considering it wasn't long ago that there weren't any meetings in Scotland at all. We hope this inspires others to start meetings in new places.

Dear *2600*:

You really need to update your listings for both the meetings and their home pages. Many are dead or have the wrong information. Also, the phone number for the payphone at the Boise, Idaho meeting has been gone for over a year, as is the payphone in Brighton, England. The phone number in Beit Shemesh, Israel can only be reached from within Israel. As for the web pages, the following meetings' links are gone: France; Los Angeles, California; and San Jose, California. Please make these corrections. It has also come to my attention that the *2600* Australia website is not a true *2600* meeting site, but a company using the name for for-profit activities at the meetings.

conscript

Thanks for the updates, most of which we had become aware of since the last issue. We've removed the non-working payphone numbers. The French website has changed to a new one and the San Jose site is back in operation, albeit not very updated as seems to be the case with many of the websites. We don't know what became of the Los Angeles website, which seems to have been taken over by another entity entirely, so that one's been delisted. None of this has affected the meetings as far as we know. Obviously, we can only update the magazine when it comes out, so it may seem like outdated info isn't being updated when it actually is. As for Australia, this is news to us. We see no evidence of anything improper. As long as the meetings are open to all and not sponsored by another entity, we don't see a problem. Our readers will certainly let us know if we're mistaken.

Dear *2600*:

Is there anyone I can call to find out if anyone is meeting at the Lenox Mall in Atlanta today? Don't want to make the drive for nothing.

Robert

We don't give out that kind of information, nor do we collect it. Meetings are very informal, so there's no way to know for sure who specifically will be there, if a huge mob will appear, or if nobody at all shows up. If we hear of the latter happening repeatedly, the meeting will be delisted. Often, all it takes is for someone to make an effort to get the word out locally. Once that happens, meetings tend to take on a life of their own.

Dear *2600*:

I am an IT student at CSUN. I had a few questions about *2600* meetings.

Do you guys still hold meetings in Los Angeles because the link to the Los Angeles *2600* meetings site appears to be for sale? Is there a newer link? If not, where do I get info about the Los Angeles *2600* meetings? Do I call in advance or do I just show up?

George

The best thing to do is just show up. Websites are notoriously outdated or not maintained. (We can't believe how many people have written in about this specific one.) Los Angeles has always had a very strong presence, so it's very unlikely you'd be wasting your time by heading over.

Dear *2600*:

Just checking in for the Petaluma (California) meeting. They are going great and increasing each month. Now that our meetings are posted in the magazine, I hope to have more people showing up. We're having great conversations on security and projects, and we have a server on Discord where we hold discussions and people post articles. Feel free to join. We are trying to find a better location to have the meetings downtown, so we might have to change our meetings in the magazine. Is that something that is possible? Thank you and hack all the things.

Mad Glitcher

It's definitely possible, but we advise that you be absolutely certain before deciding on a move since additional changes can cause confusion that lasts far longer than you might expect. As we only publish quarterly, our listings won't reflect changes for up to three months, so it's important that any change be one that's considered permanent, or at least one that won't change again for a while. Once more, having a local website that attendees can check makes this so much easier. Best of luck to this new meeting.

Dear *2600*:

I would love to get a group going in central Arkansas. I have a lot of background in PCs and networking. I have a few certifications and at this time am perusing my degree in network security and cyber security. I would love to talk with people that I can learn from and can learn from me.

Carl

We think you meant "pursuing" and not "perusing" but we thought we'd leave that in case you were conveying another message. While we have a meeting already in Ft. Smith, another in a different part of the state certainly couldn't hurt. Please know that you won't be judged based on your certifications, skill, jobs, or anything other than your attitude. Best of luck.

Dear *2600*:

No meeting in Fargo that I could find at West Acres. Closest thing was the hacking coughs from the geriatric crowd. I brought my magazine for bait, but no bites.

Fritz

Naturally, we'll delist it if this continues. But hopefully people will see this and band together to try and save this meeting from extinction. Fargo needs this.

Dear *2600*:

I'm one of your subscribers from Italy, I'd like to know what are the requirements in order to organize a meeting in my city for it to be printed on the last page of the magazine?

Cristy

We've sent you the guidelines so you should have everything you need. All we can advise is to be patient and diligent. It can sometimes take a while to get people to show up, particularly in places where the magazine isn't prevalent. But hackers aren't know to shy away from a challenge.

Taking Action

Dear *2600*:

Get them. You don't need permission. You do need to be angry at the Russians for their interference on *all* levels Go get them. Do your best.

Terry

Hold on there, Rambo. What exactly do you expect us to do when we "get them?" Take over their Facebook pages? Turn off their electric grid? Hack their elections?

If the allegations being thrown around turn out to be true, we have nobody to blame but ourselves. Attempting to manipulate elections is what countries have always tried to do to each other. Our own country has probably done it to everyone at some point. We should have expected it, we should have recognized it, and we should have taken more steps to prevent it. Having a little cyberwar to settle the score isn't going to accomplish anything, other than making hackers look like some sort of military tool.

But it's not all bad. We're learning an awful lot about manipulation, revisionism, and propaganda. We're finally getting that crash course in world history we needed so much.

Dear *2600*:

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

R

Or you could do a story about the things that are on your blog and reach people who would never know about you otherwise. If you believe the story is only about you, well, good luck with that. We intend to stick with the issues.

Dear *2600*:

I'm a writer and academic from Idaho. I'm writing because I've long wanted to purchase the entirety of *2600* for a writing project, and I was curious if you'd be at all interested in portions of it. My plan is basically to start from the very beginning, and chronicle my experience of reading all the way through, including occasional quotations with citations of where they're coming from. Obviously, this would be a huge endeavor, but I've loved *2600* for a long while and always hoped to write something to honor that. The basic framework will likely just be a blog, which I'll send your way of course, but then I'm hoping to write snapshots that reflect where things have come from. I just wanted to see if this struck you as interesting and worthwhile. The end goal would, of course, be a book, perhaps on the order of "My Year(s) with *2600*," utilizing the constraint of the project to incorporate personal material and my overall interest in the mag and its subject matter.

Anyway, I just wanted to check as I will be purchasing the haul and starting soon.

G

You certainly don't have to check with us to get going on this project, but we appreciate the acknowledgment. As we told the previous writer, the story shouldn't be about just one person or entity, and that includes us. It sounds like you know what you're doing and we look forward to seeing what you put together. Good luck!

Dear *2600*:

Since the "Free Kevin" movement, we've come a long way for an ISDN and DSL connection. Now look at us! Kevin's out, Bernie's out, and where the fuck is Phiber Optik in 2017 (don't hate - I haven't followed your whole fucking show)? Miss him on the broadcast. Things have changed. I don't like it.

Open IP and route... if you want to find me, you can. Thanks for the shirts! Fuck Trump! And keep up the good work. I'll be listening as long as I can. I'll continue to throw money at your show.

P.S. Stay away from politics and stick to technology. Unless you can keep your political rants under 20 minutes.

An Avid Reader/Listener (~93)

Change is good when you have a say in it. We've definitely accomplished a lot over the years. We see that in looking over our own archived annual digests every three months. We have no idea who you are and don't intend to track you down. But we appreciate the support and advice. We hope not to get mired in political rants, but rather to link various worlds together so that we don't become alienated from any of them, and so our readers and listeners are able to find relevance in a whole bunch of unexpected places.

Dear *2600*:

Hello 2600.com Team

I need your help to hack the website https://[redacted].com/ because this website harmed me in past life and I have requested them lots time to remove it, but they are not accepting my request. So I really need your help to hack this website. Can you please help me? If you don't want to share with me your strategy, please hack it on your end. I will be very grateful to you. Once you have hacked the website, please send me the confirmation mail.

David

We had enough to mock you for without seeing a second email from you, but this one had the greeting of "Hello Hackaday Team" instead. So you basically sent this letter out to anyone with half a clue who might be able to perform this service for you? Nice.

We have absolutely no interest in being your digital mercenaries for your perceived injustice. People say all kinds of things on websites. There's often little to nothing you can do about it. If someone is committing a crime, then there are ways of dealing with that. But to expect a bunch of hackers to just solve these alleged problems by hacking a website is a severe oversimplification, no doubt aided by a fixation with bad television and stupid movies. You need to move on and not worry about what's on a damn web page somewhere. That kind of thinking can literally grind civilization to a halt.

Thanks at least for not offering to pay us for this service. That would have only added insult to naïveté.

Inquiries

Dear *2600*:

A pentester and I have got together to collaborate on an article providing advice to those looking to get into the ethical hacking industry. Both of us provide recommendations to those looking who want to share on a wider scale as there isn't enough good advice for those wanting to get into the industry.

Would you be interested in such an article? If so, I can send you the final version next week. We haven't published it anywhere else.

R

While we'll certainly look over anything that's sent to us, we have to advise you that this whole "ethical hacker industry" concept isn't really something that sits well with us. Sure, hackers can find places in all sorts of industries using their skills and their individual talents. But commodifying it into its own industry with grades and classifications - not to mention the implication that hackers aren't by default ethical - really doesn't feel right in our opinion. That said, we're always open to different views and, if you feel our readers might gain something from your perspective, we'll definitely give your piece consideration.

Dear *2600*:

As many folks are well aware, most cell phone companies allow you to purchase insurance to replace your phone in the case of accident or loss. What many folks probably aren't aware of, however, is that a single company, Asurion, handles many of the replacements and is a complete pain to work with. I recently lost my phone on a camping trip and I had to speak to three different Asurion agents before I could have them input a correct address for delivery because, for whatever reason, my mobile carrier (Cricket) would not allow me to change my address in store, and they were required to send you a code via text in order to do it online. This caused nothing but frustration for me, so I figured I would try to make it easier for folks who find themselves in a similar bind. Whenever I would call the Asurion number they provided me with to speak to an agent in regards to my phone, it would allow me to enter my number, but then would only provide information about the tracking number associated with the package, never allowing me the opportunity to speak with an agent. I kept trying numerous attempts to dial 0 for an operator, as well as speaking "Operator" or "Customer Service" but to no avail. I eventually called this number: 1.888.881.2622 and ended up punching in my parent's old landline and trying to start a replacement claim on it before it would allow me to connect to an agent. Once there, I explained to the agent my troubles with updating an address for replacement delivery as well as provided them with the actual phone number that required service. Though they were very nice and accommodating, they still managed to mess up my address further, and failed to provide an apartment number for delivery. Do any other readers of *2600* have similar experiences with Asurion or have any tips or resources for people who have to deal with them in the future?

Thanks for all the great tales. I felt like for the first time in years that I had successfully pseudo social engineered my way through the phone and it was very rewarding.

J

It's ironic when you have to social engineer your way into your own account to get something that you're entitled to. We've heard numerous experiences of a similar nature with Asurion and, quite frankly, the whole thing seems like a scam to us. If you calculate how much you pay them for insurance plus your deductible versus what it costs to actually buy a new phone (assuming you don't get some sort of deal from your cell phone company or find a decent used model through a third party), the numbers tend to not add up in your favor. And if you use them twice in a certain period of time, you'll get dropped. We also found it weird that if you lose your phone, they'll send you a replacement (of their choice), but if your phone breaks, they will charge you the full price of your phone if you don't send it to them in a certain period of time. When you add in the privacy implications of sending your phone to them; there seems to be no disadvantage to saying it was lost no matter what. Of course, that leads us to people who try to take advantage of this for their own purposes, which we don't condone. But completely destroying a broken phone rather than risk having your private data fall into the wrong hands is something we have no problem with. In the end, even without the hassles you experienced, this just doesn't seem like a worthwhile expense. We're curious if others feel differently.

Dear *2600*:

I'm considering writing an article about bringing the book cipher into the 21st century. It could end up being a series of articles, with the first one being a discussion of the requirements one might see necessary.

Before continuing, though, I want to make sure this would be new information.

While I've been a lifetime subscriber for many years, I've been remiss in my reading. In the past few days, I did gain access to the PDF files. Unfortunately, as you know, not all of the issues are in digital format and many are scanned images and thus can't be searched (easily).

Can you, please let me know about issues/articles dealing with cryptography, especially (but not exclusively) the (1) book cipher, (2) stream cipher, or (3) moving the book cipher into the 21st century?

Thank you for your time and consideration.

Bertram

You're welcome to our consideration, but we can't be as generous with our time. Even though we publish the thing, going through and gathering every article that deals in any way with cryptography would take far more time than we've got. You can scan the titles of every article we've ever run by looking at the back issue selection on our store, but that won't include anything that was mentioned in the letters. We can say that nobody here recalls an in-depth article on these subjects in recent memory if that helps you at all. (We know that stream ciphers have been mentioned in passing from time to time.) But even if we had run something on this exact subject, your perspective would undoubtedly be different, and that's the kind of thing that we're after. Just because someone's mentioned a certain topic doesn't mean that there's no room for additional discussion or more ideas. So by all means, write about this and send it on in. We hope to make it easier to get our issues into searchable form and increase the number of platforms they're available on. First, we have to finish getting them all into digital formats, which has been a massive undertaking that is nearing completion.

Dear *2600*:

I have bought the audio-only DVDs from every single one of the HOPE conferences. I'm wondering what your policy is on file sharing. Is it possible to share the old ones and not necessarily the new ones? Which ones can I share? I'm not making any profit out of this, I just want some of my friends to listen to the audio. Thank you for your time.

Warmfuzzy

We have absolutely no problem with people sharing not only the audio, but the video from all of our conferences. We only ask that you let people know where it came from. The same goes for the magazine. We want all this info to get out, after all.

Dear *2600*:

I have a Caller ID problem. When I want to active it's gray out. How to fix it.

SS

Wow. Did you really expect us to be able to figure this out with what you told us? Solve the communication problem first and then come back with a question that makes sense. Are you trying to send or receive Caller ID? Be sure to include what device(s) you're using and what exactly you're trying to do. It would be super helpful.

Dear *2600*:

Can you accept donation for the less privileged?

Kiraz

A little context would sure go a long way here too. Unless you're sending us a telegram, words are free and should be used in abundance to illustrate your point.

Dear *2600*:

The 2600.com and YouTube channel *2600* is good. but can I know because I trust on you. Is earth is really flat?

heavenligible

And then there are times when even context wouldn't really do much good.

Dear *2600*:

Kind of an odd question for anyone willing to answer. Was flipping through the Spring issue and in the back in the Shout Outs section, I was shocked to see the name "Kitten Academy." The importance of this is that I was watching the very same livestream while reading! Is there some sort of hacker/kitten connection? I'm sitting here in astonishment of this seemingly cosmic coincidence.

Dumbfounded,
Phil

While it may seem like an amazing coincidence, the fact is that kittens help to provide sanity and we've never needed more of that in our lives than now. The good folks at kitten.academy deserve our support and thanks for making everything more bearable just by allowing us to watch life unfold. We don't doubt there are numerous other examples of this. We'd love to hear about them.

Dear *2600*:

I'm a reader of *2600* and full-time producer, artist, and chaser of curiosity. I am writing to request information on the next issue's theme with the intention of submitting for the *2600* Summer issue cover. I am capable of composing digitally (via Photoshop) or creating an illustration.

Ambitiously,
Jack

We appreciate your ambition, but we generally put the covers together in-house. If you have specific ideas of your own, please share some of them and we may contact you. Either way, please continue to create and share. We all need more of that.

Dear *2600*:

I used to buy *2600* from Tower Records in Dublin, Ireland years ago. I went in recently and asked the young lad behind the counter where I would find it. Needless to say, the look on his face like I just took a shite in his kettle was enough for me to know he hadn't a clue what I was asking for. Any reason Tower Records stopped stocking it?

Dave

It's interesting in itself that Tower Records still exists in Ireland (Japan too) even though it went bankrupt in most places more than a decade ago. As to why they don't carry us, that's a very good question. Overseas distribution is a real challenge, as it's expensive to ship and many places aren't particularly open to foreign publications. We're looking for suggestions on how to help fix that.

Article Responses

Dear *2600*:

Got three years of back issues recently. This time, I'm not trying to read more than one issue a night! Dave Maass had some really good points in this article "EFFecting Digital Freedom: Defending Privacy on the Roads" in 32:4. This automated plate recognition stuff drives people like me crazy. I had heard about some guys in Florida that deliver pizza getting those "Dear John" letters from the state. One guy posted that he almost got a divorce because of one of those letters. Sucks because when you work in the pizza business, you don't exactly get to choose where you have to drive.

The Dev Manny saga has gotten really interesting, I'm hoping that wasn't the last installment in this issue. Guess I'll find out tomorrow!

Also, I have a question for anyone who might know. I had a crew out today installing a black Q-tip looking thing on top of a pole that a traffic light hangs from in front of an apartment building. I've looked around and determined that this is either a milli- or centi-cell (smaller than a cell, bigger than a micro-cell), some kind of surveillance equipment, or a speaker/warning device of some sort.

E85

Thanks for the feedback. The EFF column is always informative and the continuing Dev Manny story definitely has a number of us riveted. As for your mystery device, a picture would definitely help. In fact, maybe we should start another feature called "What Is This?" since there are so many bizarre devices popping up lately.

Dear *2600*:

Response to "How To Improve Zone Protection In Burglary Alarms" from 34:1: Cezary Jaronczyk's article talked about how to spoof voltage levels in a circuit to bypass burglary alarms. The main idea is that a burglary alarm, which works by putting a certain voltage on a line, can detect an open door when that voltage changes. This assume the mechanism detecting the open door shorts out resistor R1 when the door is closed and puts that resistor back in when the door opens. However, the circuit presented there doesn't work.

The schematic shown comes with no good explanation but as best I can figure, the op-amp is supposed to put the "correct" voltage back on the rail after the door is opened so that the alarm measurement side (the lower rail or pin 2 on J1) can't see any transition. However, the op-amp circuit is not connected right. The switch to the capacitor needs to be connected to Wire 2 so it learns that voltage, since it is that voltage which gets measured by the burglar alarm. The output of the op-amp needs to be connected to the same wire, not pin 1 on J1. Connecting it as shown will make the op-amp dump the original voltage on to the circuit upstream from R1, but then when R1 enters the voltage divider, it'll cut that voltage down, which is what we want to avoid.

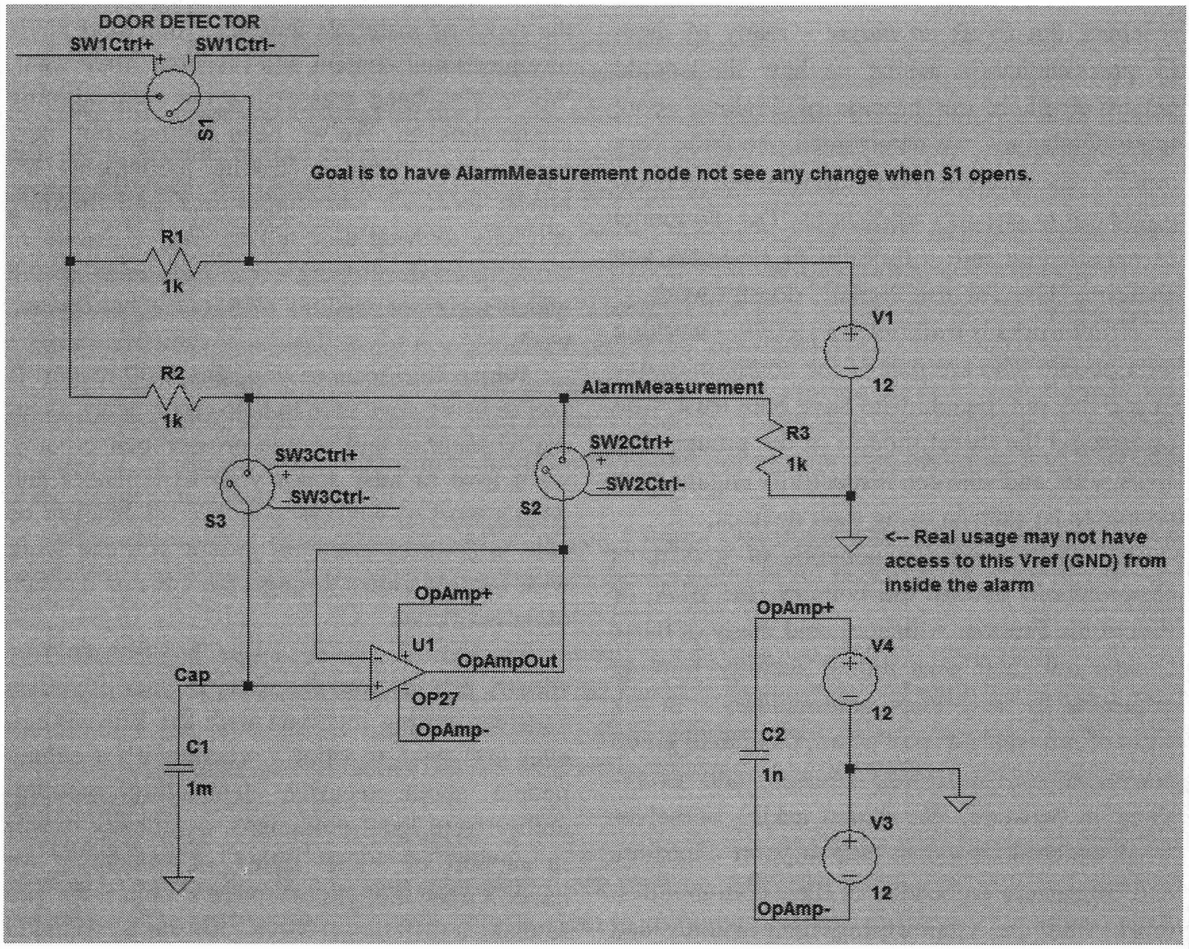
Another way to say that is that the voltage on Wire 1 will not change when the door is opened, since it's on top of the voltage divider, so it shouldn't be worried about. It is the detection voltage on Wire 2 that counts, so we need to spoof that.

This assumes that the hacker can attach the ground of the circuit to the same ground as the burglar alarm (perhaps by connecting the chassis together). If the hacker can't do that, then reversing the connections from what is shown may work better, using Wire 1 as common and Wire 2 as signal output from the op-amp. This is because Wire 1's voltage won't change in either state (door-closed and door-open), so it makes a good common reference.

In the last part of the article he purports to have a design which cannot be bypassed with the previous method. His idea is to have the voltage level change randomly, so it can't be spoofed. However, the idea behind the first circuit is still valid: a voltage-follower op-amp can be used to read the voltage on the low side (the signal), and replicate whatever it is supposed to be, thus cutting out the door-open detector. Depending on what op-amp the hacker uses, an extremely fast response time can be created easily, which could match the speed of any zone detection circuit.

The schematic shown in Figure 3 is even more confusing and mangled than the one shown in Figure 2. That last schematic has a number of bogus connections and neither of those last two images gives meaningful information to an informed reader.

Monican



Goal is to have AlarmMeasurement node not see any change when S1 opens.

<-- Real usage may not have access to this Vref (GND) from inside the alarm

EFFecting Digital Freedom

Building Digital Safety Skills in Your Community

by Soraya Okuda and Elliot Harmon

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

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

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

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

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

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

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

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

BUILDING A BETTER SCREEN LOCKER FOR GNU/LINUX

by idk

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

Deficiencies of Modern Screen Lockers on Desktop GNU/Linux

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

Goals

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

Materials

slock

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

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

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

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

xssstate

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

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

GPG

`https://www.gnupg.org`

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

EncFS

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

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

grsecurity

`https://grsecurity.org`

We use grsecurity in a slightly custom

configuration in order to make it possible to prevent USB attacks that attempt to brute-force our screensaver by emulating a Human Interface Device. The configuration available to Debian Sid/ Jessie-Backports works well with one config-only modification.

Other Things To Note

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

Creating Our Password and Data Store

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

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

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

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

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

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

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

Example Wrappers for GPG

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

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

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

Init Scripts

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

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

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

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

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

Modifying slock

First, add the following pre-processing options:

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

Next, create the USB lock functions:

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

Now, add the GPG/EncFS lock functions:

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

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

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

at the top of unlockscreen (around line 480):

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

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

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

Configure Settings

Modify /etc/sudoers:

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

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

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

For USB enabling/disabling:

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

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

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

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

to

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

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

In Conclusion

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

ACK

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

CITIZEN ENGINEER

by ladyada@alum.mit.edu and fill@2600.com

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

Patently Hacking

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

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

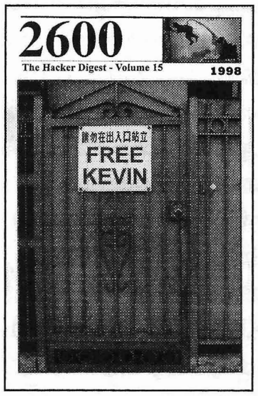
Another recent SCOTUS decision relevant to any hacker or tinkerer, as well as people who repair things, came only a week later. On May 30th, the Supreme Court decided on the case "Impression Products, Inc. v. Lexmark International, Inc." The case involved a toner-cartridge-refilling company (Impression)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

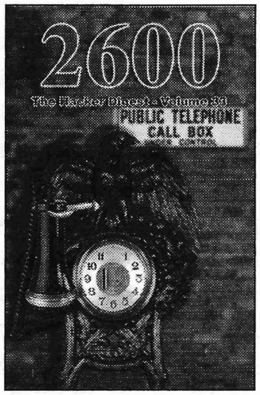
One of the judges used this example: *"Take a shop that restores and sells used cars. The business works because the shop can rest assured that, so long as those bringing in the cars own them, the shop is free to repair and resell those vehicles. That* *smooth flow of commerce would sputter if companies that make the thousands of parts that go into a vehicle could keep their patent rights after the first sale."* - Chief Justice John G. Roberts Jr.

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

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

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





VR Trumpers

by Jeffrey H. MacLachlan

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

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

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

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

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

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

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

Above all, I was able to temporarily experience the mind of Trump supporters. You cannot reason with them because they lack the ability to comprehend reality beyond their immediate sensory input. Global warming will permanently damage the planet? Well it's cold outside, so how is that true? The economy is strong? Well, the only Dollar Store in town just closed down, so how is that real? The majority of Americans actually voted for Hillary? Well, everyone I know voted otherwise, so that must be a lie. I loathe making any lazy *Matrix* allusions, but there is no spoon indeed. The most important thing you learn in higher education is how little you actually know. Public schools do not expose students to humanity's greatest thinkers. There are no semesters devoted to Nietzsche or Baldwin or Marx, and so you default back to what you personally experience for intellectual guidance. Through automation and globalism, many rural spaces now resemble a dystopia, and according to a recent Heartland Monitor poll cited in *The Atlantic,* Americans born in rural areas are significantly less likely to move away from home than their urban counterparts. So it shouldn't be too much of a shock that a television character was able to use the medium to marionette the weak minded into pulling a lever for tyranny. If you have never mentally or physically moved beyond what you know, you cannot understand the complexities of reality.

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

Successful Network Attacks - Phase Three

Gaining Access

by Daelphinux

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

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

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

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

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

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

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

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

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

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

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

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

Advice from the Socially Engineered

by Infra Read

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

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

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

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

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

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

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

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

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

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

Internet Thoughts

by Jared J. Estes

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

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

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

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

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

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

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

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

by Andy Kaiser

Chapter 0x13

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

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

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

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

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

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

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

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

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

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

"That still sounds vague."

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

"That's not much to go on."

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

"Sounds fun."

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

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

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

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

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

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

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

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

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

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

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

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

"No kidding."

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

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

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

"Yep."

"Tell me you're running a keylogger."

She smiled. With her teeth.

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

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

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

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

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

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

P@nic shrugged.

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

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

HACKER HAPPENINGS

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

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

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

August 6-7
Maker Faire Tokyo
Big Sight
Tokyo, Japan
makezine.jp/event/mft2016

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

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

October 21-22
Ruxcon
CQ Function Centre
Melbourne, Australia
www.ruxcon.org.au

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

November 3-5
PhreakNIC 21
Clarion Inn
Murfreesboro, Tennessee
phreaknic.info

December 1-3
Maker Faire Rome
Fiera di Roma
Rome, Italy
www.makerfairerome.eu

December 27-30
Chaos Communication Congress
Congress Center Leipzig
Leipzig, Germany
www.ccc.de

July 20-22, 2018
The Circle of HOPE
Hotel Pennsylvania
New York City, New York
hope.net

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

Marketplace

For Sale

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.

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

HTTP://CRYPTOBIZ.DIRECTORY. Show the world your professional side: profile page, email address, and phone number with voice-mail. And we're not profiting from selling your info. We collect micro-payments for the services you use, as you use them.

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.

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.

Announcements

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!

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.

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

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/

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

Services

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

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/

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

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.

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.

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

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

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

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

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

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

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

Personal

GOT TORPEDOED OUT OF THE REAL WORLD, living in the Fed world now. Looking for U.S. and worldwide correspondence on all topics. Interest in encryption/cryptography, Constitutional violations, Infosec, esoteric thinking. Looking forward to hearing from friends new and old. Kevin Reynolds #59650-018, FCC Coleman-LOW, P.O. Box 1031, Coleman, FL 33521.

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

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

Deadline for Autumn issue: 8/21/17.

WANT TO BECOME A DIGITAL SUBSCRIBER TO 2600?

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

Head to digital.2600.com for the latest

ATTENTION WRITERS

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

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

ATTENTION LIFETIME SUBSCRIBERS!

If you want to receive annual digital digests instead of - or in addition to - your quarterly paper issues, this is now possible without having to buy both at full price. For $100, we will sign you up for the lifetime digital digest plan as well (once we verify that you are an existing lifetime subscriber). You will receive all of the digests that have already been released (Volumes 1-15 and 25-33) plus five newly released ones each year, and one per year once all of the back issue digests have come out.

Just visit the downloads section at store.2600.com and sign up!

"Truth is stranger than fiction, but it is because Fiction is obliged to stick to possibilities; Truth isn't." - Mark Twain, 1897

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Infrastructure
flyko

Network Operations
phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Roger Waters, Omar Santana, Sneaker Pimps, L'Orchestra Cinematique, Angelo Badalamenti

Shout Outs: The Washington Post, The New York Times, The Guardian, the Committee to Protect Journalists, and Freedom of the Press Foundation

Welcome: Leopold

***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);
Summer 2017, Volume 34 Issue 2, 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: Bodegon Bellagamba, Carlos Calvo 614, San Telmo. In the back tables passing bathrooms.

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: Oxford Scholar Hotel, 427 Swanston St.

Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

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

BRAZIL

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

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm

Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.

Vancouver: International Village Mall food court.

Manitoba

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

New Brunswick

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

Newfoundland

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

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA

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

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECHIA

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

FINLAND

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

FRANCE

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

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

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

THAILAND

Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM

England

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm

Leeds: The Brewery Tap Leeds. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), front entrance on Coventry St. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Bell Hotel Pub, lower floor near the TV. 6 pm

Scotland

Edinburgh: Rose St, between 1780 and Dirty Dick's.

Glasgow: Starbucks, 9 Exchange Pl. 6 pm

Wales

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

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

Arizona

Phoenix (Mesa): HeatSync Labs, 140 W Main St. 6 pm

Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Tucson: Sunny Daze Cafe. 6 pm

Arkansas

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

California

Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (business park behind the thrift store). 7 pm

Chico: Starbucks, 246 Broadway St. 6 pm

Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar. 6 pm

Monterey: East Village Coffee Lounge. 5:30 pm

Petaluma: Starbucks, 125 Petaluma Blvd N. 6 pm

Sacramento: Hacker Lab, 1715 I St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Center near street level fountains. 6 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

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

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

Delaware

Newark: Barnes and Nobles cafe area, Christiana Mall.

Florida

Fort Lauderdale: Grind Coffee Project, 599 SW 2nd Ave. 7 pm

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Jacksonville: Kickbacks Gastropub, 910 King St. 6:30 pm

Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm

Sebring: Lakeshore Mall food court, next to payphones. 6 pm

Titusville: Bar IX, 317 S Washington Ave.

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

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

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance.

Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Space by Doejo, 444 N Wabash, 5th floor. 6 pm

Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.

Indianapolis: City Market, 2nd floor, just outside Tomlinson Tap Room.

West Lafayette: Jake's Roadhouse, 135 S Chauncey Ave.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Davenport: Co-Lab, 627 W 2nd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

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

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Michigan

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

Minnesota

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

Missouri

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

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

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

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm

Las Vegas (Henderson): Las Vegas Hackerspace, 1075 American Pacific Dr Suite C. 6 pm

Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Somerville: Dragonfly Cafe, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 6 pm

New York: The Atrium at 875, 53rd St & 3rd Ave, lower level.

Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

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

Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).

Raleigh: 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: Emma Inc., 11 Lea Ave. 6 pm

Texas

Austin: Dobie Mall food court. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm

Houston: Ninfa's Express seating area, Galleria IV. 6 pm

Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont

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

Virginia

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm

Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington

Seattle: Cafe Allegro, upstairs, 4214 University Way NE (alley entrance). 6 pm

Spokane: Starbucks, Hawthorne Rd.

Tacoma: Tacoma Mall food court. 6 pm

Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.

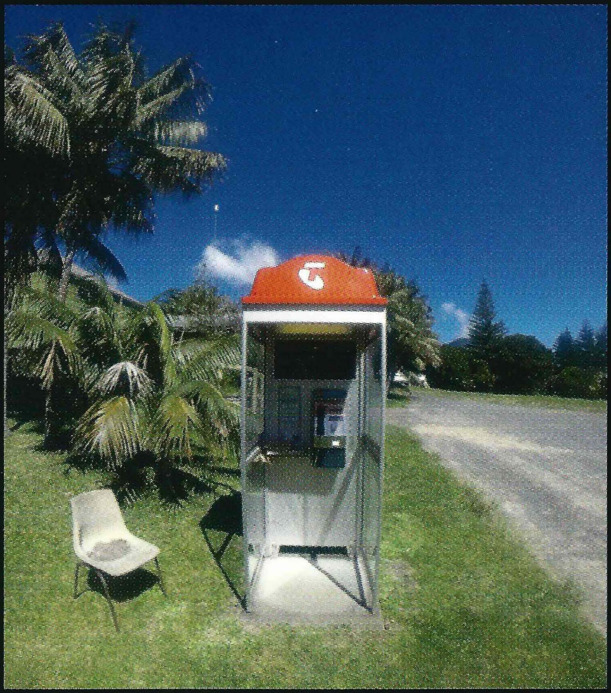
Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

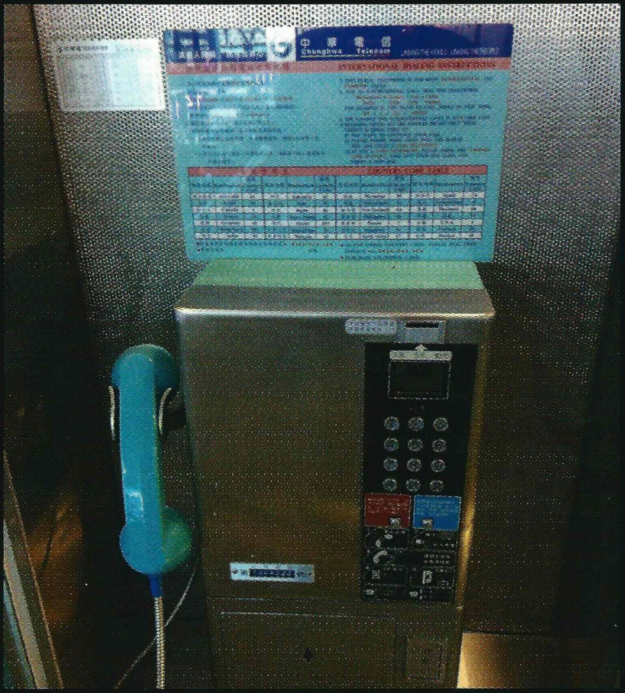
All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

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

Payphones of the East

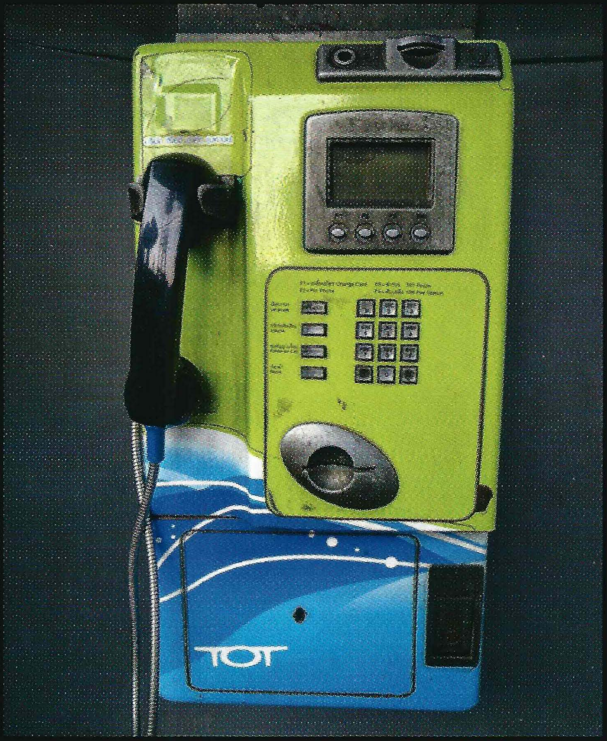


Australia. This is one of only two payphones on Lord Howe Island. This one was near Joy's General Store and it even comes with a chair. (The other payphone is at the airport.) ***Photo by Greg Sherman***



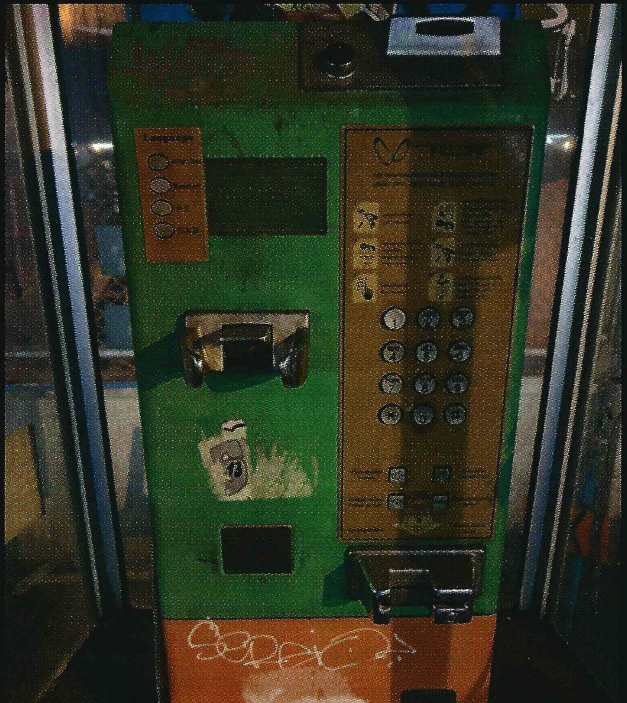
Taiwan. Spotted at Taoyuan Airport near Taipei, this phone seems way bigger than it needs to be. We're surprised someone hasn't stuck a big ad on all that empty space.

Photo by Justin Davis



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

Photo by Sam Pursglove

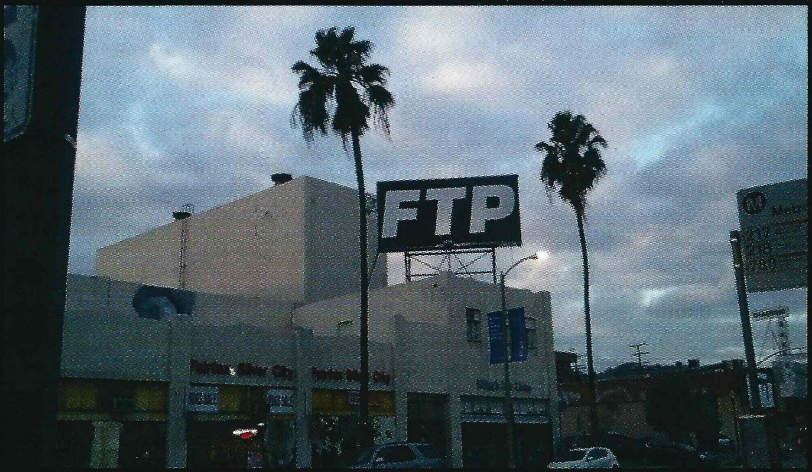


Thailand. Another aesthetically pleasing model, this one found in Phuket. The colors offset themselves perfectly, making it possible to admire while completely missing the fact that it has no handset.

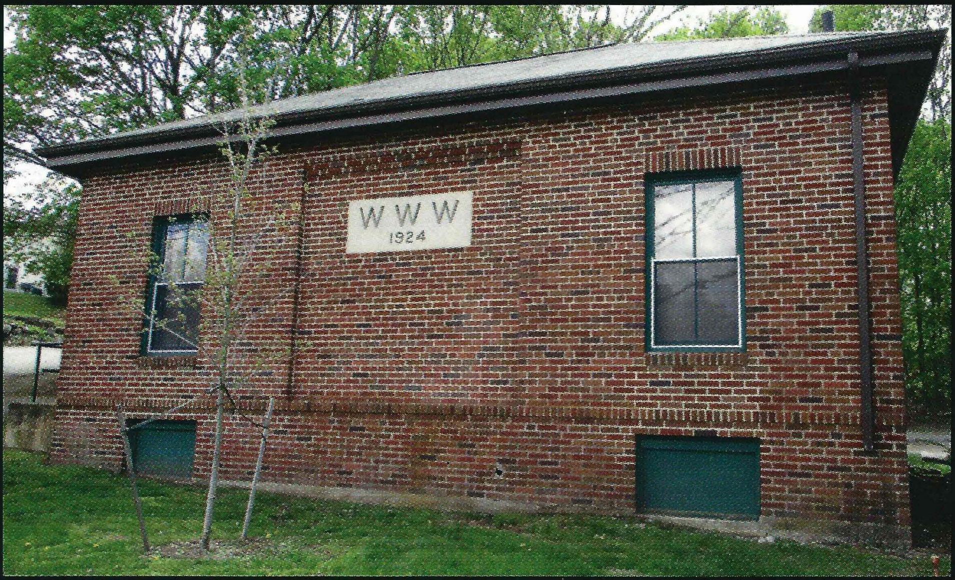
Photo by Sam Pursglove

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



A little known fact: all FTP transfers go through this building near the corner of Fairfax Avenue and Beverly Boulevard in Los Angeles. At least we assume that's the case - it would explain most of the bottlenecks we experience. Discovered by **SC**.



This must be the building that housed the very first website back in 1924, another little known fact that you'll only find on our back cover. Thanks to **Barry von Tobel** for findng this piece of history in Waltham, Massachusetts.

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.