

**Volume Forty-Two, Number One!**

**DIGITAL EDITION Spring 2025**

# 2600

**The Hacker Quarterly**





# Payphones With Color



**Poland.** Found in Poznan, this is actually a restored phone booth from the 1960s which no longer has a phone in it. Instead, this is an informational kiosk where visitors can listen to recordings of eyewitness accounts of the June 1956 uprising which took place here.

*Photo by ZENIAL*



**Ireland.** This phone booth has more color and overall architectural integrity than many entire buildings. Seen in the village of Ballintober in County Roscommon.

*Photo by Banríon*



**Saint Lucia.** This red classic is still in use and in good working order. The people in the capital city of Castries rely on this daily outdated technology to make cheap calls, instead of the cellular services offered by the same company.

*Photo by Allan Reid*



**Hungary.** The pink, blue, and silver are pleasing to the eye while the working dial tone is pleasing to the ear. Found in the Buda part of Budapest on Castle Hill.

*Photo by jon.18*

Got foreign payphone photos for us? Email them to [payphones@2600.com](mailto: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 (Do not send us links as photos must be previously unpublished.)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)



# SIGNS

this will happen again

Attitude Control	4
Using Prediction Error-Inspired Insights to Tackle AI Bias and Hallucinations	6
Brute Forcing a Website Passkey by Spoofing Web Authentication Using cURL	8
Red Tape and Bureaucracy - That's What's Wrong With Us	9
Meditations on Societal Collapse (Via Payphone)	10
The Perception Lens	11
TELECOM INFORMER	13
Hackers in Hospitals	15
Setting Up a Simulated Environment for the Robot Operating System (ROS)	16
Who Authors Unauthorized Access?	19
Am I Still a Hacker if I Use an LLM?	20
Building a Password Cracker Using OpenAI and Rust	21
Nine Censored Haiku	25
HACKER PERSPECTIVE	26
Zero-Day Markets: Inside the Shadow Economy of Exploits	29
The Changing Definition and Practice of Privacy	31
How I Learned to Stop Critical Thinking and Love Security Defaults	32
LETTERS	34
EFFECTING DIGITAL FREEDOM	46
What is the Hacker Ethic - Redux	47
Take Me Out to the Reverse ATM	49
ARTIFICIAL INTERRUPTION	52
The Cult of Youth	54
A Timeline of Recent Search Engine Events	55
Cybersecurity Can Be Expensive	57
I Took the Red Pill: A Journey to Linux	58
Lee Williams, Harassment Agent Episode 5	59
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

# Attitude Control

None of us can say we're surprised. We knew this period in history would be filled with controversy, destruction, and pain. It's been all of that and more.

But what many failed to predict was the unprecedented takeover of government institutions by the mysterious Department of Government Efficiency (DOGE). Within days, this organization (not a department of the government, despite its name) seized control of multiple government agencies, firing employees and accessing sensitive computer systems.

On February 1st, DOGE gained access to classified information of the United States Agency for International Development (USAID) without security clearance. Elon Musk, the unelected, unvetted, and unconfirmed head of DOGE (a position that has been both admitted to and denied on multiple occasions), declared "we're shutting [USAID] down" before crucial aid to developing nations was terminated and employees dismissed. One ex-worker described it like this: "In a matter of hours DOGE shut down our websites, took over email handles, and summarily removed the system access of hundreds of gainfully employed public servants." That's right, the people who were vetted and had legitimate access to computer systems and sensitive data were locked out and fired by people who weren't cleared and didn't have legitimate access. In what world would this not be a cause of great concern?

Similar stories played out at the Consumer Financial Protection Bureau (CFPB), the Department of Agriculture (USDA), the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention (CDC), the Department of Health and Human Services (HHS), the National Oceanic and Atmospheric Administration (NOAA), the Department of Energy (DOE), the Social Security Administration (SSA), the Federal Emergency Management Agency (FEMA), the Internal Revenue Service (IRS), the Federal Aviation Administration (FAA), the Department of Veterans Affairs (VA), and even the National Nuclear Security Administration (NNSA) and the Department of Defense (DOD).

Now, we've had differences and concerns related to just about every one of these organizations over the years. Hackers have always believed in revealing examples of security weaknesses, harmful policies, criminal activity, and outright fraud. Oftentimes, the only way to get this

information is to have someone on the inside reveal the truth - or to gain access through a security hole. And whenever something like that happened, hackers would inevitably be maligned as the biggest threat to Western civilization. The revelation itself would almost always be completely lost as the media, authorities, and general public fixated on the methods with which the information had been obtained.

What is happening here is far more insidious, as access is being seized through force by the government itself. Agencies and departments are being targeted as if their very existence is a potential threat. Much of this can be traced to personal vendettas or a desire to upend the institutions that we have come to depend upon. In addition to possessing all the hallmarks of a major security breach, this bears many characteristics of a coup from within.

We welcome transparency in government organizations whenever possible. People certainly deserve to know the truth behind where their tax dollars are going and what policies are being carried out in their name. Eliminating waste and fraud is a laudable goal when done in a competent, fair, and open manner.

However, none of that appears to be happening here. DOGE has tried to operate in complete secrecy. When *Wired* revealed the names of some of DOGE's employees, Musk himself threatened them with prosecution. Apparently, the people are not entitled to know who is behind the biggest takeover of federal agencies in our nation's history.

Fortunately, this Soviet-style tactic of intimidation and obfuscation didn't hold. We, along with many others, felt compelled to track down and add more details and more names to the list and spread it throughout social media, including on Musk's own Twitter (X). The number of people who stepped up and helped spread this publicly available information was in itself inspirational. It didn't stop what was going on, but it let the world know that we weren't going to be intimidated - and we certainly weren't going to be quiet.

Of course, this was such a trivial part of the entire operation. These mysterious people (many of whom were either still in or barely out of school) were affiliated in various ways with Musk and most had absolutely no experience working in the government. That meant they had no clue what they were looking at and predictably



weren't able to make informed decisions on budgetary or policy changes. This quickly became apparent the moment reporters started to analyze what it was they were actually doing. The media shared many examples of alleged savings being wildly miscalculated, misinterpreted, or just outright lies. The new regime's response to this was to categorize the media as enemies of the state, and to try and intimidate or restrict them into submission. Meanwhile, DOGE quietly and without comment began erasing its many inaccurate claims and figures, ostensibly to make it seem as if they never existed. But again, this doesn't work in the face of freedom-minded and fearless individuals and institutions. archive.org has been performing one of the greatest public services of our age simply by archiving government websites that are being wiped or changed. They're not alone. What DOGE and their kind are learning is that you can't hide from the past, especially with an efficient team of web crawlers.

While there is much courageous behavior we can salute, there has also been a disturbing amount of cowardice, most notably in the tech sector. Where we had once hoped for these companies and the billionaires behind them to stand up for freedom, diversity, anti-hate, inclusion, dissent, etc., we have instead seen them bow down to the powerful entities that have a vested interest in silencing opposition and propping up corruption and fascist ideologies. As we said at the beginning, none of us should be surprised by this. It only goes to show that those with money and power rarely also have integrity. They live in fear of losing what they have - or even losing a small amount. Don't look to them to do the right thing or to lead. You will always be disappointed. Instead, use their resources against them. Technology is an ally. Unbridled power is a threat.

Incredibly (and especially on the platforms run by those we criticize), we find *ourselves* accused of supporting a corrupt system and even "the government," apparently by people who haven't taken a look recently at what the current government is. There are those who believe that because much of what we describe is due to the actions of someone who's technically proficient, we should by default be supportive. That's not how this works. We love technology, innovation, and diving into systems as much as anybody. But we also recognize the threat posed by someone with an agenda who *knows* what they're doing, as opposed to that posed by someone incompetent who can easily be outsmarted. And we will never follow someone blindly just because we're impressed by their credentials. We will

always have questions and - as we see so often today - when questions become the enemy, it's a huge red flag.

There is no administration we have not criticized or whose victims we have failed to acknowledge. But because they are all guilty doesn't mean they are all the same. What is currently taking place (and we can only imagine what else will have happened weeks from now when this issue is released) is so far removed from historical precedent as to be almost impossible to compare. What *can* easily be compared to the past is today's willingness of a part of the populace to go along with whatever they're told, despite obvious evidence to the contrary. "Freedom of speech" is supposedly part of the new way, unless you say something critical or challenging, in which case you're punished. "Cancel culture" is over, unless you disagree with the party line, in which case you are purged. If we somehow were to find ourselves on the side of those who wielded power in this manner, these tactics would be so disturbing to us that we couldn't possibly remain there. And we know there are many who are in that exact position now, and are being turned off to something they once saw hope in. They must be welcomed and not judged if the rest of us are to have any chance of turning all of this mayhem around.

As for DOGE's actions, the damage is likely irreparable. We will never know how compromised our private and sensitive data has become. We'll never be totally sure that there aren't back doors and trojans planted throughout government computer systems. To blindly trust those who were given unfettered access on a whim is about the most foolish thing we can do. In fact, there are even members of DOGE who had a history of such actions, yet were still allowed access. This is an injury that will be afflicting our nation for years, if not decades.

We encourage people to stay strong and to know that you're not alone in your frustration, anger, and fear. While the "opposition party" has been pathetic in its response to all of this, we think of that as evidence that good ideas have yet to come forth, meaning any one of us may come up with one, based on our ingenuity, individuality, knowledge of technology, and understanding of history.

This is about as dark as we have seen it get - and we've seen a lot of darkness over the years. But one shining beam of light is the hacker spirit, where we rise from wreckage and despair and figure out a way to build something better, something not prone to bugs and failure. We're ready for the challenge.



# Using Prediction Error-Inspired Insights to Tackle AI Bias and Hallucinations

by Jackson Mershon

I want to start by saying that I find hallucinations troubling.

That being said, imagine if your computer could learn from its own mistakes in real time - like a system that's constantly fine-tuning itself, much the way our brains do. In a world where digital systems are increasingly intertwined with every aspect of our lives, the idea that machines might self-correct, adapt, and even defend themselves isn't just a cool theory - it's a necessity. Drawing on insights from neuroscience - especially the concept of prediction error - this article explores a vision for AI that continuously adjusts its behavior, mitigates bias, and prevents hallucinations before they become a liability. For those of us in the hacking and cybersecurity communities, this isn't just academic - it's about understanding how systems can be both exploited and defended in real time.

I've spent a fair amount of time reading about how the brain deals with surprises - when what you expect doesn't match what actually happens, your brain fires off error signals that drive learning. Consider auditory mismatch negativity: when a series of familiar tones is suddenly interrupted by an oddball, your cortex responds immediately with a distinct electrical signal. Researchers like Garrido, Kilner, Kiebel, and Friston (2009) have mapped these responses through the brain's layers, showing that top-down predictions and bottom-up sensory inputs are in a constant, dynamic conversation. The key takeaway? Real-time corrections happen the moment an error is detected.

Now, picture an artificial neural network built on similar principles. Instead of processing inputs in static batches and then later updating weights with backpropagation, every layer of the network would continuously evaluate its own prediction error:

$$\varepsilon(t) = x_{\text{observed}} - x_{\text{predicted}}$$
$$\text{epsilon}(t) = x_{\text{observed}} - x_{\text{predicted}}, \varepsilon(t) = x_{\text{observed}} - x_{\text{predicted}}$$
, and trigger immediate adjustments when this error exceeds a dynamic threshold:  $\theta(t)$ .

This isn't too far-off - it's an approach

that could give continuous learning and real-time adaptation. From hackers/explorers and defenders alike, the notion of a self-tuning system is both tantalizing and open with opportunity.

At the core of this approach lies Karl Friston's free-energy principle. In simple terms, living systems strive to minimize "surprise" by constantly updating their internal models to better predict incoming data. Mathematically, free energy is expressed as the sum of a negative log-likelihood term and a complexity term via the Kullback-Leibler divergence. For engineered systems, maintaining a low free-energy state means the AI is always aligning its predictions with what's coming in from the real world. Sure, this continuous adaptation might demand extra compute power, but what's the alternative? Stagnant models that can't keep up with a rapidly changing environment are an open invitation for exploitation.

Let's talk applications. In many real-world scenarios - whether it's complex classification tasks or natural language generation - traditional models retrain only after days or weeks, by which time biases or inaccuracies might have already festered. An error-driven system, on the other hand, could monitor live outputs and recalibrate on the fly. Imagine a language model that begins to generate off-track or factually dubious statements. A mismatch function, defined as:

$$\text{Mismatch factor} = 1 - K(s)$$
$$\text{Mismatch factor} = 1 - K(s)$$
, where  $K(s)$  measures the consistency of a statement  $s$  against a trusted knowledge base, would immediately flag any deviation. When the mismatch factor exceeds a certain limit, the model would pause and recheck its output before finalizing it. This real-time check could be a game changer for preventing hallucinations.

The promise of continuous self-correction opens a new frontier in what may become "AI wars." In today's cyber battleground, adversaries are constantly probing systems to extract internal details. A self-adapting AI that exposes its error thresholds might inadvertently



broadcast hints about its internal state. How much internal data is too much? How much can you trust the user and their ignorance?

Picture an attacker who systematically feeds carefully crafted inputs, gauging the system's responses. Every borderline trigger, every near-threshold event, becomes a clue. Over time, an adversary could design inputs that nudge the model's parameters, slowly warping its definition of "normal" operation. A system that's constantly adjusting could be coerced into accepting patterns that it wasn't originally designed for.

On the flip side, these same adaptive signals can serve as forensic breadcrumbs for defenders. Repeated near-threshold triggers are like alarms going off in a network - they tell you someone is probing the system. It becomes a cat-and-mouse game: as attackers learn to fine-tune their approaches, defenders can inject unpredictability into the thresholds. One effective strategy is to add a controlled dose of randomness:

$$\theta(t) \leftarrow -\theta(t) + \gamma \omega t, \quad \theta(t) \leftarrow \theta(t) + \gamma \omega t,$$

where  $\omega t$  is a small, unpredictable noise term.

The stochastic tweak makes it significantly harder for an attacker to reverse-engineer the AI's internal state, keeping the defense robust even under sustained probing.

This interplay of adaptation and vulnerability raises a host of provocative questions. How do we balance transparency - needed for self-correction - with the risk of revealing too much to potential adversaries? What ethical issues arise when systems both expose and conceal their operational states? And can a constantly evolving AI maintain the reliability we require in critical applications, from financial systems to national security?

The implications extend beyond technical performance. In domains such as financial fraud detection, intelligence analysis, or even digital art forensics, a system's ability to adjust on the fly can be transformative. Every self-correction leaves a trace, however - a potential target for those looking to exploit the system. It's a delicate balance, reminiscent of the ongoing tug-of-war in cybersecurity, where each defensive innovation often invites a counter-innovation from the offense.

Integrating neuroscience principles into AI is not merely theoretical - it is a practical strategy for enhancing both reliability and security. By emulating the brain's continuous error detection and immediate correction mechanisms, AI systems can adjust in real time to unexpected deviations between predicted and observed outcomes. This ongoing calibration helps mitigate biases and prevents the emergence of hallucinations, ensuring that the system remains robust in dynamic and unpredictable environments.

A framework based on real-time error monitoring, dynamic thresholding, and controlled stochastic adjustments provides tangible benefits in countering system vulnerabilities. With each discrepancy promptly addressed, the approach not only improves accuracy but also serves as a defensive measure against adversarial inputs. Although such continuous adaptation may demand additional computational resources, the trade-off is justified by the enhanced resilience and integrity achieved, especially in scenarios where security is paramount.

As digital threats become increasingly sophisticated, adaptive AI isn't just a concept - it's a necessity. By continuously monitoring and correcting errors in real time, these systems can neutralize vulnerabilities before they escalate, fundamentally altering the dynamics of cyber defense.

In this evolving landscape, every exploit, every misstep you orchestrate, becomes an opportunity for the machine to learn and fortify itself. The challenge, then, is not just about finding a flaw but outsmarting an opponent that adapts with every move.

As adaptive AI learns from every exploit, how will you craft your next move in a game where the rules are rewritten in real time? Will your logic be sound?

### Sources and References

Garrido, M. I., Kilner, J. M., Kiebel, S. J., & Friston, K. J. (2009). Dynamic causal modeling of the auditory mismatch negativity. *Biological Cybernetics*, 100(3), 259-274.

Rao, R. P. N., & Ballard, D. H. (1999). Predictive coding in the visual cortex: A functional interpretation of some extra-classical receptive-field effects. *Nature Neuroscience*, 2(1), 79-87.



# Brute Forcing a Website Passkey by Spoofing Web Authentication Using cURL

by ZU1PH3R

When my friend asked me to penetrate his Jellyfin media server, I had anticipated a brute force attack should be the first method I would use in an attempt to break down the walls hiding all of the freshly uploaded anime and video game soundtracks. What I hadn't expected was encountering a secondary authentication method outside of the regular passkey I would be trying to find. This is where I was introduced to web authentication. Web authentication is a process that verifies a user's identity before allowing any further authentication to continue. In Jellyfin's case, it needed to authenticate my web client as well as my device ID in order to continue with the authentication process. This would not be an issue if I simply went to my friend's website and manually typed in each password guess I had on the main portal, but this brute force method is time consuming and non-reliable.

This is where cURL comes in. cURL, or Client URL, is a command line based tool that allows for users to transfer and request web data, such as authentication and file transferring. A simple cURL password attempt could look something like this in a terminal:

```
curl -x -H "Content-Type:
applications/json" -d
'{"user":"foo","pass":"bar"}'
http://exampleNetwork.net:1234/
login
```

This posts an http request to the server which carries the json packet holding your authentication information to the login page. This will either validate (200 status code) or invalidate (401). In the case of Jellyfish, this will *not* authenticate even if the credentials are correct. This is due to the lack of any web authentication and/or a malformed http request. The server needs to authenticate your identity which it is unable to do if you are not giving it any client information, such as what browser you are using. That is where the wonderful world of http headers comes in. Headers carry extra information that an http request might require. In the example above "Content-Type" is a header, preceded by the self proclaiming -H (header) flag. This header's purpose is to tell the server that the data I am trying to post to it is in json format. Fortunately, we are able to abuse headers and spoof the web authentication headers that the server needs in order to authenticate the client. In a simple example that is done as follows:

```
curl -x -H "Authorization:
MediaBrowser Client="Jellyfin
Web", Device="Firefox" -H
"Content-Type:
applications/json" -d
'{"user":"foo","pass":"bar"}'
http://exampleNetwork.net:1234/
login
```

This will now tell the server that the request is coming from a Firefox browser and *not* from a command line client, or null client. It's important to note that this is not a full header example for Jellyfin's web authentication, but it exceeds at giving an example on how spoofing the authentication headers can let a user web authenticate using cURL. In order to avoid malformed requests and obtain the necessary headers, one would need to perform an authentication request; an attacker can utilize Inspect Element on the website. To do this, an attacker simply needs to view the http requests between them (or someone else they want to spoof from) and the server after attempting a password on the actual website portal. Most web browsers should let anyone copy this request as cURL, doing all of the command line work for an attacker. Now an attacker has the necessary authentication headers in order to brute force the password. Once I figured all this out, I now needed a way to actually automate the attack! First, I converted the cURL command to a Python function using a cURL converter, which are easily available on the web. I then wrote the brute force script by supplying the now Python http request function, then spamming those requests by using a variable for the password header, which would loop through rockyou.txt until the password was found.

While this method can circumvent web authentication, it also has a few drawbacks. A decent firewall would be able to see the request spam coming through and block all requests coming from that IP, or even lock the main account altogether. It also does not support anonymity since you do have to fork over some type of valid web authentication, but this can be easily fixed by spoofing someone else's web authentication headers. This brute force method also takes a *long* time, since it has to go through the Internet. I was able to brute force "1234" for the password in roughly seven minutes, which is considerably long once you realize how high up on the rockyou.txt 1234 is.

In conclusion, spoofing web authentication headers allows for an attacker to continue to brute force password and web authenticated websites by abusing http headers, allowing for an automated script to be run. This can also work on other forms of authentication that are handled in the http request such as any tokens one might need. While my friend *did* have to reduce the server's firewall for this attack to work, the adrenaline from gaining access and having all the new media on my hands was well worth it.



# Red Tape and Bureaucracy - That's What's Wrong With Us

by Bluefossil

In the Autumn 2024 issue, Ig0p89 asks us what's wrong? Why are people leaving cybersecurity? Why is the supply of qualified and skilled cybersecurity professionals dwindling? Is it a lack of passion, desire, interest? Absolutely not. AI and automation? Maybe just a little, but no, that's not the main issue either. The author goes on to suggest that political forces likely play a large part in this challenge. I am here to both confirm and compound on this theory.

Ig0p89's experience with a county municipality closely mirrors my experience working in a very similar capacity with a city municipality. If people had any clue what goes on in their local governments... anyway, I digress. Let's stay on topic. Being responsible for the network security infrastructure of a city with a population of over 250,000 people was quite interesting at times. Not only was I responsible for securing public library kiosks to prevent malware, city attorney PCs, city judge and courtroom PCs, but also a full 911 call center and all public safety departments, including police and fire, just to name a few. When I first took on this responsibility, I was amazed to find that those public library kiosk PCs had direct SMB access to improperly configured file shares the courtrooms across town had configured to share docket information between attorneys and judges. So much for privacy. (I wish I was making this stuff up.)

Children would often find creative ways to bypass group policy and change desktop wallpapers or do any number of other stupid things to the public kiosks. When we headed down a path to properly secure those systems, you would not believe the amount of pushback received from library staff. Something as simple as URL filtering to prevent accessing pornography was met with objection. After all, adults must be able to use public resources to access any Internet resources they desire. We literally had to set up "adult access" kiosk stations in a separate section of the libraries where adults could request unfiltered Internet access to get their pornography fix while at the public library. After all, what else is the Internet for if not porn and cats? (I wish I was making this stuff up.)

The police stations and officers were some of the worst when it came to bureaucracy. Side

note - ironically, laptops, desktops, and other IT equipment was over three times more likely to get "lost" if assigned to the police department than *any* other department throughout the entire city. Briefing room PCs had to have access to *Candy Crush* (I guess to provide officers with a way to de-stress while on break?), and God forbid you block a patrol officer's access to any website. Yes, we had divisions that worked on sex trafficking, child pornography, and other horrendous crimes and yes, they needed access to Tor, the deep web sites, Craigslist, and wherever else, but I never understood why the motorcycle patrol needed to be able to access Netflix. (I wish I was making this stuff up.)

For every attempt to secure the network and minimize risk, there was always an equal and greater rebuttal to leave everything alone. Whether it be department heads, city manager, or even city council, I could never enact even the most basic of security best practices without a fight. I thought it was just this dysfunctional city. Then I moved into the security vendor space working for a global organization supporting SLED (State, Local, and EDucation) customers and boy did I quickly find out that it wasn't just my city that was dysfunctional - it was *every* city, county, and state municipality, and don't even get me started on the education space.

The good cybersecurity professionals know what needs to be done - and know how to make it happen, and in many cases, *do* make it happen, only to be hit with red tape and bureaucracy and directed to undo it all. Then, when the malware infects, the files get encrypted, or the library patrons start printing out confidential court documents, who do you think gets blamed?

It's no wonder we get burned out. Many of us are super passionate about the industry. I don't know about you, but I still get extra excited at every opportunity to perform a red team engagement. But red tape and politics will only allow you to get so far before you get burned one too many times, and start considering a new role in auto mechanics, welding, or plumbing (all trades where we can still use our logical minds and troubleshooting skills). Oh and by the way, pin-to-pin messaging is not an effective way to avoid open records requests!



# Meditations on Societal Collapse (Via Payphone)

by Maya Ventura

Let's consider a hypothetical.

You are in the downtown area of your local city center. You have been dropped there with absolutely nothing but the clothes on your back - no purse, no pocketbook, no phone, no keys, no change, nothing. You are in trouble. You have to reach someone you trust. You know their phone number, all you need is a phone. Asking to borrow someone's phone is pretty unlikely to work - we live in a low-trust society these days, after all. What would be the cheapest way to buy a cell phone and get it connected to a provider?

The best place I can think of for this that is likely to exist in a downtown city location is Dollar General. The best deal you'll get on a phone is for a Tracfone-branded smartphone for \$19 - for the phone. Tracfone's cheapest service plan is \$15 a month. With modern prepaid brands offered by both AT&T and Verizon, you can't just connect them to Wi-Fi and go about your day - they require activation in order to get past setup. These are subsidized devices, it's never gonna be that easy.

So right there, you're at \$34 total for a phone and service - and, of course, you can't buy a prepaid cell phone at most retailers without a valid ID, either. Looks like this entire thought exercise was pointless, eh?

Now, of course, what if I told you there was a way to make a phone call in a public place for usually just two quarters, or one dollar for long distance, or, hell, zero dollars and zero cents if you're really in a pinch and calling collect? More than that, what if I told you that these were adopted en masse, available pretty much everywhere from office buildings to train stations, and had very little downtime when paired with bare basic regular service and maintenance?

And then what if I told you we pretty much entirely got rid of this solution in favor of the previous one? You probably see where I'm going at this point. Folks: the public payphone.

Now, I'm sure some of you are thinking that the scenario I'm positing is pretty unlikely. And you'd be right! So, in order for me to make some kind of a case here, let me use a much simpler example - my old, cracked, worn-out iPhone.

I have absolutely beat the hell out of this phone. It sits at about 2.5 hours of battery life when actively in use. As a result, when I'm out doing full day trips when I'm without my car, it's often dead. It's meant I've not been able to reach people I'm picking up from various places, whether something for work, or girlfriends from the Greyhound station. Indeed,

it seems reasonable to say that transit hubs are a particularly good case for having public phones on offer - and, actually, some of Pittsburgh's light rail stations still do have them or did have them until recently. You will often find very small banks of individual public phones at airports, almost always equipped with TTY keyboards. In my experience, that's actually true in a lot of places, including at rest stops along sections of Interstate 80 (among others) - major highways being a similarly good use case, particularly for emergencies.

I actually want to talk about emergencies specifically for a minute. Once upon a time, there used to be public phones on a lot of street corners, particularly in cities. These were genuinely great for emergency cases - for both bystanders and victims, whether that's something like a car crash, or just simply being robbed... a scenario where you're quite likely to not have a phone on you for rather obvious reasons. In the case of ones placed in rest stops along major highways, it's also a great resource if you simply need to call AAA. When it comes to much more wide-reaching disasters, they play a similar role, as public phones often continue to operate during blackouts (a fact Verizon used to brag about). Indeed, after September 11th, Verizon installed over 220 wireless payphones in addition to the 4,000 already installed in downtown Manhattan, and offered free calls to the public through them. Not to say that 9/11s are particularly common these days, but with general weather disasters and large-scale violent acts at all-time highs thanks to climate change and the dawn of new political extremism, I think it's a reasonable point, particularly considering headlines from late last year about Elon Musk's offer of "free" Starlink Internet access in areas affected by Hurricane Helene actually costing upwards of \$400 for equipment.

But there's actually one use case that I want to put a little more focus on, which I started really thinking about after exploring some of the resources available at my local library - people without housing.

This is where the prepaid cell phone pricing I mentioned earlier in my implausible hypothetical comes into a real-world scenario. There is a significant population out there that simply can't afford or access that for one reason or another - cost or lack of necessary documentation. Even as cell phones get more affordable over the years, there's still a pretty significant barrier for someone with no income, particularly considering being in poverty is also

highly correlated with not having access to a current ID. The Carnegie Library system here in Pittsburgh is actually very accommodating towards folks without access to an ID - offering membership to Allegheny County residents pretty much automatically as long as there is an electronic record of them residing there, and accepting pretty much anything with an address on it otherwise. They also offer career training opportunities, voter registration resources (a voter registration card actually being enough to get library membership, coincidentally) and computer access, on top of being a fee-free library system overall, making the whole library system an extremely good resource for underprivileged folks. However, the CLP main branch in Oakland has one resource that surprised me: an actively maintained payphone. That phone is actually what got me thinking about their potential utility to underprivileged communities - after all, it's a lot easier to get two quarters than it is to pay for a whole phone - as well as the general population at large simply just for convenience and accessibility.

But despite everything, telecom giants - namely AT&T and Verizon - are pretty gosh darn uninterested in maintaining infrastructure like public phones, regardless of the societal benefits,

because it absolutely is not worth the investment in terms of capital. Verizon and AT&T's decision to depart from the public phone industry and just abandon existing infrastructure, despite it having next to no direct impact on their bottom line, is depriving us of a valuable resource in service of an additional half of a decimal point on their annual reports.

And that's what all of this represents - a public service, unfairly painted as obsolete due to decrease in usage, totally decimated by major corporations, with every opportunity to save it, whether in recent history or 50 years ago, being missed. It sucks for everyone involved and we're worse off as a result.

To wrap this up, we're never going to see a resurgence of public telephones in this country. We've let go of something useful because corporations told us we didn't need it anymore. Denial of communication has long been a tactic used against undesirable populations, and the only people who are going to put up a fight against it are those of us in the hacker communities. We can't do much, but with luck, hopefully we will help to establish a new era of communication, one in which reaching out is not only desirable, but mandatory.

## The Perception Lens

by aestetix

In July of 2012, after years of struggling to get any press coverage, the HOPE conference faced a strange dilemma: we were getting flooded with press requests, likely due to featuring recent NSA whistleblower William Binney as the Friday keynote. The nascent press "team" consisted of myself and the late Cheshire Catalyst, who had decades of experiences dealing with public image issues. On the day before the conference started, we realized that we had to come up with a way to let press identify themselves, and quickly. Otherwise a whole slew of problems might follow. The badge that year was a hacker passport - in line with the theme "Department of HOPEland Security" - and the passport came in a plastic sleeve that connected to a lanyard. We realized that we could take the conference logo, which happened to be a mockery of the DHS logo, and add some words to it to make the "press pass" look legitimate. We could then print up copies of the "press pass" in the guest computer lab in the hotel lobby and slip the sheets into the badge sleeves. After some brainstorming,

Cheshire came up with the perfect phrase for the words: "perception lens."

To understand why this phrase is so fitting, we should recount a brief history of press relations. We can all likely agree that the public trust in the mainstream media is at an all time low - otherwise why would there be such a surge in independent outlets and podcasts? But has it always been this way? What is the relationship of the press to power, and to the people? And why should hackers care?

We have traditionally referred to the press as the "fourth estate," a notion borrowed from 18th and 19th century English politics. Americans modified it to complement the existing three branches of government. If we have a separation of powers by executive, judicial, and legislative, then granting power of public opinion to the press by way of the First Amendment creates yet another separation, a further check on power. The most famous example of this in modern times is probably the reporting by Bob Woodward and Carl Bernstein on cover-ups in the Nixon



administration, which ultimately helped lead to Nixon's resignation. In the following decades, however, the shared commons between the press and government have evolved into a shared bedroom, and the press is far more reluctant to publish hard-hitting pieces, lest they lose privileged access into the halls of power. For example, *The New York Times* withheld stories about the Bush administration's warrantless wiretapping in 2004 until after the election was over. This nepotism seems to have encouraged more renegade groups like WikiLeaks to obtain documents of public interest and then publish them, sidestepping the *quid pro quo* agreements into which the mainstream media has entered with government.

We should note that the love relationship between press and power has ebbed and flowed over time. In his 1987 novel *Empire*, Gore Vidal describes with some viciousness corruption among the newspaper moguls like William Randolph Hearst. A similar sentiment echoes through movies like *Citizen Kane* and *His Girl Friday*. Therefore, nearly a century later, we are yet again at a nadir in this relationship, where the established press seems to care more about itself than those whom it claims to serve. Unlike in the 1980s, when Operation Sundevil led the Secret Service to raid computer systems hosting BBS servers, or in the 1990s when Kevin Mitnick was thrown in jail without a trial, contemporary journalists cannot claim ignorance on how technology works. Most newsrooms will have a dedicated IT staff, or at least someone knowledgeable enough to set up and maintain SecureDrop, which means that, rather than clueless reporters trying their best to keep afloat of complex stories, there is downright malice and hostility towards common sense as news outlets publish propaganda puff pieces that maintain an undeserved status quo.

Consider the recent developments where Luigi Mangione, a young Ivy League computer science graduate, has allegedly assassinated the CEO of UnitedHealthcare. Rather than pursuing the public interest and trying to answer important questions (How was an amateur lone wolf able to escape from the most surveilled city in America? Why did someone with so much going for him give it all up? Why is so much of the public in support of this alleged murderer?), they

focus on irrelevant details, such as the rich CEO's surviving family. They also lavish the NYPD with undeserved praise, ignoring the fact that the police didn't have a name for their suspect until a lucky break came in from another state. As of this writing, not a single reporter has asked the NYPD why the invasive surveillance system didn't catch Mangione, and whether taking away so many people's right to privacy has resulted in a better society. Instead, cable news outlets like CNN and Fox News serve up five to ten minute "interviews" with talking heads repeating the same vacuous platitudes about how murder is wrong, and none of them wanting to talk about the big picture before they "run out of time." Is it any wonder then, that people are unplugging their cable lines and tuning in to hours-long podcast discussions instead?

All too often, hackers will dismiss a current event as unimportant unless it impacts them somehow, like the Kevin Mitnick saga. To an extent, this is reasonable. If the news of the day involves a random celebrity peacocking about and creating random drama, it's likely no more important than an episode of reality television. But we need to recognize when there is a shift in the zeitgeist. The media has evolved from concerned citizens ignorant of tech but faithful to a journalistic mission, into government and corporate puppets with varying degrees of maliciousness, whether they be parroting statements from their overlords or actually serving as judge, jury, and executioner to character assassinate an unwitting victim in a sham trial masquerading as an interview. Their role has morphed into gatekeepers who aim to quell an angry public, rather than truth-seeking inquisitors.

The questions we ask powerful entities and the responses they give help form the tapestry of information which allows us to distinguish truth from nonsense. The way we describe an event, the style in which we read or listen to a story, and the facts which we include or exclude, all play into Cheshire's perception lens. Like a camera or telescope, this lens can be used to clarify or to distort. If power controls it, they can modify narratives, dictate stories to the media, and keep normal people in check. But if access to this lens is democratized, and power is held accountable for how closely the narrative comes to matching truth, then the press might once again live up to its title as the fourth estate.



# TELECOM INFORMER



by TProphet

Hello, and greetings from the Central Office! Today I'm in the Turan neighborhood of Turkistan, Kazakhstan. Why, might you ask? It's a long story involving a Lada and a cat named Murka. But let's back up to 2021, when I first intended to do this project, and ended up in Dubai a few months later instead. There was a pandemic, borders were closed, and there were more projects in major cities than there was capacity. These days, as the economy worsens in the United States, smaller international projects are finally back in the picture.



*Turan neighborhood, Turkistan, Kazakhstan*

If you have never heard of Turkistan, it's in southern Kazakhstan along the Silk Road and about 300 kilometers north of Tashkent, Uzbekistan. If you didn't know better, you'd think you were in eastern Washington because the terrain looks very similar. It's an historically important place, with a famous mausoleum built in 1399. And it's growing like crazy. Starting around 2020, Turkistan built a giant shopping mall; airport terminal; modern supermarkets; a 3D flying theater; a new regional capital, parks, hotels, you name it. The development happened at a speed and scale that I have really only seen elsewhere in Chinese cities, creating truly world class infrastructure out of the desert. Although the development was a pet project of the former president of Kazakhstan and had a high risk of

becoming a white elephant, the massive level of investment seems to have paid off. Turkistan has a small but growing tourism industry, and the regional government relocated its offices there as well. It has become a regional center of government, tourism, and commerce.

All of this means more people, more infrastructure, and more demand for bandwidth. You might not exactly expect a place like Kazakhstan to be as wired as it is, but it's a society that highly values science and technology and is willing to invest in it. After all, the space program of the former Soviet Union was centered there, and the Baikonur Cosmodrome space complex (leased by Russia and supporting the International Space Station) still operates. Kazakhs are just as online as people in North America, or perhaps more so.

Turkistan, however, was starved for options until recently. In neighborhoods with fixed line telephone service, Kazakhtelecom offered ADSL service for residential Internet. Mobile carriers offered 3G and 4G service, with levels of quality ranging from terrible to just OK. The mobile carriers offered residential solutions via portable hotspot or USB modem plans, but with slow speeds, data caps, and questionably reliable service. There is also a local satellite TV provider called Ottau TV, but unlike some U.S. providers, they don't provide satellite-based Internet services.

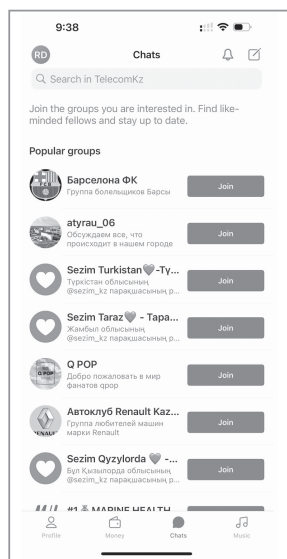
The landscape has quickly changed. Wireless providers are now offering 5G, although the quality of residential service offerings still isn't great given that services are chronically oversubscribed. Kazakhtelecom now offers fiber to the home in some areas, in addition to ADSL. The ADSL service is only sold with a land line telephone included and operates at slower speeds. Fiber to the home is sold at a promotional price of about \$8 per month for 300Mbps service, including a bundled streaming TV offering.

Most importantly, Kazakhtelecom probably has the most bizarre mobile app of any I have seen from a phone company (except, perhaps, Global YO). Complete pricing and service information is only available if you



download the mobile app, and the app includes a chat feature. One chat has what appears to be 12-year-olds recording audio clips of themselves singing. There are also chat channels full of lonely guys looking for love. There is an entire section full of Kazakh music videos, and a payments app. This appears to be in partnership with an app called Aitu (aitu.

io), which states that it “does not process requests related to private chats” in the Illegal Content section. Do with that information what you will.



*Possibly the most baffling phone company app I have ever seen*

If you can manage to wade your way through the thicket of “Super App” offerings, Kazakhtelecom offers a tool to check whether service is available at your address. However, the addresses they serve are limited and a significant portion of the city of Turkistan lacks service, including the Turan neighborhood. This is a largely residential neighborhood, and because of that has been long overlooked by utility services. Paved roads and a sewer system recently came to the neighborhood (although running water and electricity have been available for decades), and now fiber to the home is available through a company called DomaLine.

DomaLine is a local ISP with around 10,000 customers. Their fiber infrastructure is aerial, riding on the same infrastructure as electrical connections. Like the competition, they sell a streaming television package, offering 70 channels. This is paired with 50Mbps, 100Mbps, and 200Mbps service offerings in a range from \$12 to \$20 per month. The upstream provider is TTC, one of the larger backbone ISPs in Kazakhstan. Overall it’s a pretty reasonable setup, using brand new equipment.

At least, it *would* be a reasonable setup if

not for a cat named Murka. The nearest utility pole to today’s installation address (formal addresses are a relatively new thing in the Turan neighborhood) is located across the street. We need to do an aerial drop, and doing that requires throwing the cable onto the roof. In this neighborhood, people have tin roofs, so we don’t want to be throwing rocks. Instead, we attach the cable to a small bag of sand, and toss it across to land on the roof.

Unfortunately, Murka is on the roof, the roof is very steep, and he thinks this is a game. We toss the cable, and he knocks it down. We toss it back up, and he knocks it down again. This could go on all day. “Does anyone have any kitty treats?” I asked. Someone offered a thermos of tea. “Kitties don’t drink tea,” I said with exasperation.

There was only one solution. I found some string, one of the other guys found a feather, and we fashioned an irresistible toy. “Murrrrrrrka!” I said, slowly swinging the string in a way that was sure to attract his attention. I then began dragging it across the yard, slowly then faster, and bringing the laser focus of a ferocious hunter. We heard a clatter as he clambered off the roof, and in a tabby flash he violently



attacked the string in a hail of teeth and claws. “Now!” I said, and the crew threw the cable while I made a friend. Another 100Mbps of service was installed.

*A defiant Murka after mischief*

One of the things that I continue to observe is that countries which Americans would consider developing or mid-level developed are building newer infrastructure, in many ways leapfrogging what is available in so-called “developed” countries. At my home in The Exclave, I can barely get 25Mbps of service at over three times the cost. Fiber to the home service tiers in Turkistan, Kazakhstan starts at double that speed.

And with that, it’s time to pet Murka. Take good care of your pets, and I’ll see you again in the summer.

# Hackers in Hospitals

by Gary Rimar

aka Piano Guy

AKA head of PianoBarCon (at a cybersecurity conference near you)

Getting old isn't for wimps. Falls aren't for wimps either, especially when a fall ends in a broken ankle with torn tendons (first MRI). After months of not healing all the way, we decided it was time for another MRI, especially since having hit the catastrophic maximum for insurance (it was a bad year) the MRI would not cost me anything.

I didn't normally go to the hospital system that the orthopedic surgeon worked at because they were the most expensive place in town. Since it was "free" (at least to me), I decided this was a better way forward. My appointment was on the Saturday after Christmas.

When I went to get into the area, the first thing they did was ask me for a facial recognition scan. I asked why this was necessary, and they said "to make your name tag, to prove you've checked in." I told them I was opposed to a facial recognition scan. They called over a manager, she briefly looked at (did not electronically scan) my driver's license, and they found out that they could make me a badge without doing a facial recognition scan.

Off to the MRI appointment.

If you've ever had an MRI, you know they tell you to leave jewelry at home. They don't say to leave all other valuables at home (phone, wallet), but at this place they probably should have. The lockers in every other MRI facility would be easy enough to pick with a pick set, but that assumes someone is carrying their picks and knows what to do. In this hospital, they use the Kit-Lock KL1000. Pictures can be seen at [www.codelocks.us/kl1000-g3-kitlock-locker-lock](http://www.codelocks.us/kl1000-g3-kitlock-locker-lock). As I was about to put my phone

in this locker, I wondered if there was a bypass combination in case someone forgot their self-set combination. It took me under a minute to find out that the bypass combination is 1-1-3-3-5-5-7-7. I could have had everyone else's valuables, but among the reasons that I'd never do that is that when I'm dressed in orange I look like a pumpkin. Kidding aside, I'm very honest and ethical. When I did talk to the person who took me back for the MRI, I said "do you know the combination to get someone back in if they forget theirs?" She said yes, and it's all over

the Internet (she knew this too). I asked why they used such insecure locks. Her answer was "why do you think we tell people not to bring jewelry?"

If you've never had an MRI, they make sure you have absolutely no ferrous metal on or in you, then put you in a tube that has extremely strong magnets and can measure how your body resonates to the strong electromagnetic pulses. This allows the doctors to assess soft tissue. Because of the way they assess tissue from every angle (it's a three-dimensional rendition), they slide you through on a table to get every slice, and the mechanisms involved are very loud - you will be given earplugs to protect your hearing.

After the scan, the patient is supposed to pick up a disc with the images on it. The hospital system also puts the scan on their system, so the disc isn't mandatory, but it is a good idea to get for records and in case the network is down the day of the follow-up appointment. I asked for the disc at the desk when I was leaving and was told "no, that's at the other end of the hospital." This is a big hospital complex. Going to the other end meant getting in the car and driving, or a long walk on a cold day with sleet coming down. Plus, parking was \$7 a pop in each garage. As I was walking out, I walked past the Women's Imaging Center (they have a separate one for that) and asked if they could validate my parking. I explained that I had a bad ankle (that's why I was there) and that I didn't feel it was right to have to pay \$14 for parking. I also explained that - even though I was out of the crutches and the boot - I was here for an injured ankle. She said, "I don't validate parking, but hold on" and she walked away. Five minutes later I was about to leave in frustration, but she came out of the door she walked through and handed me two parking validation bar codes. She said, "I can't validate your parking, but they can."

It was very tempting to photograph the bar codes and analyze them. I could look at the two and figure out the system. I could have created free parking at the hospital (which is where I was going still for physical therapy) but



decided not to. First, “orange.” Second, more seriously, any time I’d use one of my “free” codes, I would cause someone else the hassle of either having to pay for parking or going back into the hospital to get a better code. As hackers, just because we can doesn’t mean we should.

When I showed up at the other end of the hospital, they said my name badge sticker was defective because it didn’t have my face on it, and they asked me to make it again. I told them no, that I had had this discussion with the manager at the other end of the hospital, and that I was just here to get my MRI disc. They relented.

I was told where to go, but there was no reception person there. No one was there except for another patient who was waiting for someone to come out (she was still in the boot and crutches phase). I was less patient,

and since doors were open, I started wandering around the back halls of the area until I found an employee. This was definitely not a place where patients were supposed to go. When I explained why I was back there, the employee took my name, told me to sit in the chair that happened to be near where I found them, and they said they would bring me my disc in the next 10 to 20 minutes (and they did).

I will be sending this information to the president of the hospital to state that they should get a disc burner at the same end of the hospital as the MRI machine and put real locks on the lockers. I wanted to give 2600 first crack at this, so I’m writing this now. And, to not leave people in suspense, the prognosis is that I need to keep doing physical therapy (which I can do at home), and hopefully the atrophied torn tendons will regrow by May, and I’ll not have to have surgery.

## Setting Up a Simulated Environment for the Robot Operating System (ROS)

by Gazza

### Intro

As a follow up to the article titled “Introduction to the Robot Operating System (ROS)” (41:3), this article focuses on setting up an environment that can simulate a robot. Specifically, we will use ROS Noetic, which is supported until May of 2025. If there is sufficient interest, I am willing to continue this series in ROS 2, so please write in if these articles interest you. There are three different ways we can proceed at this point: bare-bones, VM, or Docker. Our preferred way, and the focus of this article, is to use a docker image. However, notes and references on the other approaches are provided below.

### Bare-Bones or VM Setup

The first approach is bare-bones (or dual boot) installation. This is feasible if you have a spare laptop laying around. Alternatively, you could also spin up a virtual machine (VM). However, unless you dedicate significant resources to the VM, the simulation may be a bit laggy or freeze<sup>1</sup>. Note that if you choose to continue with a bare-bones or VM approach, the next step is installing Ubuntu 20.04. Installing Ubuntu is outside the scope of this article, but an ISO can be found online<sup>2</sup>. With Ubuntu Focal installed, the next step is to install ROS Noetic. Instructions for installing ROS Noetic can also be found online<sup>3</sup>. It is highly recommended that you set up a catkin workspace if you have any interest in pursuing ROS after this article. It is not needed for this exercise, but will save some time down the road. The directions for installing the catkin workspace can be found online<sup>4</sup>. We will get more into the catkin workspace later, but in short it allows you to add ROS packages that are not located in the repository.

### Docker Setup

There are a few advantages of using docker for ROS development. First, it resolves the “... well it worked on my computer” issue. ROS has a lot of dependencies and keeping track of which version’s installed can be a hassle. Second, it allows for multiple ROS containers to exist on the same host OS. For example, my host OS is Ubuntu 24.04; however, I have ROS containers for Noetic (requires Ubuntu 20.04), Humble (requires Ubuntu 22.04), and Jazzy (requires Ubuntu 24.04). Third, when I end up breaking things and I often do, I can relaunch the container and I am back to coding in minutes.

Do you have docker installed already? If not, instructions can be found online<sup>5</sup>. I chose to install docker using the apt repository. For convenience the steps are provided below.

```
# Add Docker's official GPG key:
sudo apt-get update
sudo apt-get install ca-
certificates curl
sudo install -m 0755 -d /etc/apt/
keyrings
sudo curl -fsSL https://download.
docker.com/linux/ubuntu/gpg -o /
etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/
docker.asc
# Add the repository to Apt
sources:
echo \
"deb [arch=$(dpkg --print-
architecture) signed-by=/etc/
apt/keyrings/docker.asc] https://
download.docker.com/ linux/ubuntu \
$(. /etc/os-release && echo
"$VERSION _ CODENAME") stable" | \
```

```

sudo tee /etc/apt/sources.
list.d/docker.list > /dev/null
sudo apt-get update
# Install the latest version:
sudo apt-get install docker-
ce docker-ce-cli containerd.
io docker-buildx-plugin docker-
compose-plugin
# Test docker installation:
sudo docker run hello-world

```

To make life more convenient, which is often inversely proportional to security, I typically also do the post install steps: “Manage Docker as a non-root user” and “Configure Docker to start on boot with systemd”. If this interests you, then this link will help with either or both of those steps<sup>6</sup>.

There are different ways to interact with docker. While the command line is one way, Visual Studio Code also has an extension called “dev containers”. This link provides instructions to install VSCode in Linux<sup>7</sup>. However, the following command typically works for me.

```
sudo apt install code
```

The next step is to install the “dev container” extension within VSCode. Pressing “CTRL + SHIFT + x” will pull up the Extensions Marketplace. Search and install “dev containers” by Microsoft. With “dev containers” installed, the next step is to download the files “Dockerfile” and “devcontainer.json” from the 2600 code repository<sup>8</sup> (or copy from below). Both of these files should be copied to “~/Noetic/devcontainer”. Now this is where using Docker really pays off. After opening the “Noetic” folder in VSCode, click the bottom left “Open a Remote Window” button (it looks like ><) and click “Reopen in a Container”. The first time you do this, it will download everything that you need; so grab that copy of 2600 and get caught up on the latest issue. After it is finished downloading (~3-4 gb of data) and compiling everything, VSCode will drop you inside a terminal in the container. Now let’s have some fun!

## ROS

### Step 1 - Spawning a Robot in a Virtual World

Once you are at the terminal inside the container, you can confirm this by checking that the bottom left corner says “Dev Container: noetic desktop-full”. The next step is typing the following command:

```
export TURTLEBOT3_MODEL=waffle
```

There are three different versions of turtlebots: burger, waffle, and waffle\_pi. Personally, I prefer the waffle model since it is equipped with an RGB-D camera (think Xbox Kinect). This command needs to be entered into each new terminal window or you will get an error.

The next step is to run the following command, which spawns a virtual world and robot. One thing to keep in mind is that “roslaunch” also runs the command “roscore”, if it isn’t already running. This is not true for “roslaunch” commands which need to have a terminal running “roscore” to execute.

```
roslaunch turtlebot3_gazebo
turtlebot3_world.launch
```

### Step 2 - Making The Robot Move

With the virtual robot and world loaded, the next

step is to make it move. The easiest way to get the robot to move is to use the package “turtlebot3\_teleop”. The “turtlebot3\_teleop” package converts key presses to the “cmd\_vel” topic. The “cmd\_vel” topic is a “geometry/Twist” message type that directs the movement of the Turtlebot3 robot. To launch the “turtlebot3\_teleop” package we need to first open a new terminal. Do you remember what we have to do when opening a new terminal? I hope you said run, “export TURTLEBOT3\_MODEL=waffle”. With the new terminal open, and the export command executed, then next step is to run the command below.

```
roslaunch turtlebot3_teleop
turtlebot3_teleop_key.launch
```

At this point, I recommend overlaying the terminal window onto the gazebo world window. For “turtlebot3\_teleop\_key” to work it needs to have focus when making key presses. Each tap of the “w” key will move the Turtlebot3 forwarded faster and faster. The “s” key is used to stop the robot and the “x” will slow forward velocity or cause the Turtlebot3 robot to back up. The “a” and “d” keys are used to rotate the Turtlebot3 counterclockwise and clockwise respectively.

### Step 3 - Making a Map

Now that we have the virtual robot and world loaded from Step 1 and the ability to move the robot from Step 2, the next step is to have the robot map the virtual world. To make a map, we are going to use the Simultaneous Localization And Mapping (SLAM) approach. There are quite a few SLAM approaches available for us to use out of the box including: “gmapping”, “cartographer”, “hector” and “karto”. For now, we will be using the “gmapping” package. Open a new terminal window and launch the “gmapping” package using the command below. I hope you remembered to run the “export” command before launching the SLAM file.

```
roslaunch turtlebot3_slam
turtlebot3_slam.launch slam_
methods:=gmapping
```

Note that this launch file opens a new window called “Rviz”. The “Rviz” window allows you to view ROS topics in 3D. In this use case, it will draw a 2D map as the robot explores the virtual world. You can save the map with the command below. The map is in the “pgm” file format and can be opened with most drawing programs. The 2D map is called an “occupancy grid”. The “occupancy grid” is typically trinary in nature using three colors. Black is used to designate “obstacles” such as walls. Light gray is used to represent “free space”. The “free space” is defined as areas the Turtlebot3 can safely traverse and is accomplished by ray-tracing to an obstacle. The dark gray areas are “unknown” and if possible, gets converted to either “obstacles” or “free space” as the Turtlebot3 explores.

```
roslaunch map_server map_saver -f ~/
map
```

How does “gmapping” work? In short, it uses the 2D lidar on the Turtlebot3 robot. The 2D lidar produces a “laser\_scan” topic. The “laser\_scan” topic is used to localize the robot in the virtual world and generate the 2D map as it explores.



#### Step 4 - An Easier Way to Navigate

While moving the robot with the keyboard is fun at first, it quickly gets tiresome. Thus, an easier way to navigate the robot is to use “waypoints”. This can be done in the “Rviz” window using the “move\_base” package. The “move\_base” package is quite complex and this article is already getting on the longer side, so I will save the explanation for the next article. The condensed version is open a new terminal window and enter the command below.

```
roslaunch turtlebot3 _ navigation
move _ base.launch
```

It is recommended to close the “turtlebot3\_teleop\_key” terminal by pressing “CTRL + C” (in the terminal window that you want to close) so there is only one node publishing the “cmd\_vel” topic. While it is possible to use a node called “cmd\_vel\_mux” to run multiple navigation methods such as a joystick and “move\_base”, I will save that discussion for later too. With “move\_base” running in the new terminal window, click on the “Rviz” window. Along the top banner is a button called “2D nav goal”. This will convert your cursor to an arrow. On the “free space” (or light gray) area of the map, click and drag where you want the robot to go. The “click” sets the “x” and “y” position of the goal and the “drag” sets the “yaw” or orientation of the Turtlebot3 at the goal. If everything worked as intended, the Turtlebot3 should start navigating to the goal. One last thing that I would like to point out is if you plan to use “move\_base” in the future, the following sequence of launch files should be used. The main reason is that “move\_base” expects the “map” frame to be published and will complain until it is provided by “gmapping”.

```
# Terminal 1:
roslaunch turtlebot3_gazebo
turtlebot3_world.launch
# Terminal 2:
roslaunch turtlebot3_slam
turtlebot3_slam.launch slam _
methods:=gmapping
# Terminal 3:
roslaunch turtlebot3_navigation
move_base.launch
```

#### Summary

In summary, I hope this article has helped to set up a ROS environment. Also, we launched a virtual robot and world. We demonstrated two different methods to drive the robot, namely “turtlebot3\_teleop\_key” and “move\_base”. We also used “gmapping” to generate a 2D occupancy grid of the virtual world. The next article will explain in more detail what is happening here and explore localization with the occupancy grid saved in Step 3. If you get tired of mapping the Turtlebot World waiting on the next article, try mapping the Turtlebot House.

```
roslaunch turtlebot3_gazebo
turtlebot3_house.launch
```

<sup>1</sup> [robotics.stackexchange.com/questions/21651/gazebo-freezes-on-vm-after-running-roscore](http://robotics.stackexchange.com/questions/21651/gazebo-freezes-on-vm-after-running-roscore)

<sup>2</sup> [www.releases.ubuntu.com/focal/](http://www.releases.ubuntu.com/focal/)

<sup>3</sup> [wiki.ros.org/noetic/Installation/Ubuntu](http://wiki.ros.org/noetic/Installation/Ubuntu)

<sup>4</sup> [wiki.ros.org/ROS/Tutorials/Install](http://wiki.ros.org/ROS/Tutorials/Install)

```
ingandConfiguringROSEnvironment
5 docs.docker.com/engine/install/
ubuntu/
6 docs.docker.com/engine/install/
linux-postinstall/
7 code.visualstudio.com/docs/setup/
linux
8 www.2600.com/code/
9 emanual.robotis.com/docs/en/
platform/turtlebot3/simulation/
#gazebo-simulation
```

#### Dockerfile

```
FROM osrf/ros:noetic-desktop-full

# Add vscode user with same UID and GID
as your host system
# (copied from https://code.visualstudio.com/remote/advancedcontainers/add-non-root-user#_creating-a-nonroot-user)
ARG USERNAME=vscode
ARG USER_UID=1000
ARG USER_GID=$USER_UID
RUN groupadd --gid $USER_GID $USERNAME \
&& useradd -s /bin/bash --uid $USER_UID --gid $USER_GID -m $USERNAME \
&& apt-get update \
&& apt-get install -y sudo \
&& echo $USERNAME ALL=(root) NO
PASSWD:ALL > /etc/sudoers.d/$USERNAME \
&& chmod 0440 /etc/
sudoers.d/$USERNAME
# Switch from root to user
USER $USERNAME

# Add user to video group to allow
access to webcam
RUN sudo usermod --append --groups
video $USERNAME

# Update all packages
RUN sudo apt update && sudo apt upgrade -y

# Install Git
RUN sudo apt install -y git \
nano \
wget \
ros-noetic-turtlebot3 \
ros-noetic-turtlebot3-gazebo

# Rosdep update
RUN rosdep update

# Source the ROS setup file
RUN echo "source /opt/ros/${ROS_DISTRO}/
setup.bash" >> ~/.bashrc
RUN echo "export ROS_HOSTNAME=127.0.0.1"
>> ~/.bashrc
RUN echo "export ROS_MASTER
URI=http://127.0.0.1:11311" >>
~/.Bashrc
```

#### devcontainer.json

```
{
  "name": "noetic desktop-full",
  "dockerFile": "Dockerfile",
  "runArgs": [
    "--privileged",
    "--network=host",
    "--volume=/tmp/.X11-unix:/tmp/.X11-unix",
    "--volume=/dev:/dev",
    "--env=DISPLAY=${localEnv:DISPLAY}"
  ],
  "workspaceMount": "source=${localWorkspaceFolderBasename},target=/${localWorkspaceFolderBasename},type=bind",
  "workspaceFolder": "${localWorkspaceFolderBasename}",
  "mounts": [
    "source=${localEnv:HOME}${localEnv:USERPROFILE}/.bash_history,target=/home/vscode/.bash_history,type=bind"
  ]
}
```

# Who Authors Unauthorized Access?

by Daryl Furuyama

The method for picking pin tumbler locks is widely known: use a torque wrench to slightly turn the plug while using a pick to either rake or individually set the pins into place. What I find more intriguing is the implications of the existence of such a method. The very precise pressure applied by the torque wrench allows for the pins to be individually set into place by the pick. Still, it simultaneously prevents the pins from resetting after losing contact with the pick. The expected process is to use a key to synchronously set and hold the pins in the correct position before attempting to turn the plug to unlock the lock. Yet, this method disrupts the order of the expected process by first turning the plug and then asynchronously setting the pins, creating an unexpected behavior.

The existence of such a process reveals a discrepancy between the conceptual framework of how the lock works compared to the actual physical operation of the lock. The conceptual framework is that all the pins must be aligned before the plug can be turned to unlock the lock. The real-world phenomenon is that imprecision in the construction of the lock allows the plug to be turned slightly without the pins first being aligned in their proper location. The tolerated play of the object allows it to enter into an unnamed third state of neither locked nor unlocked, holding the pins in stasis until they can all be manually aligned.

Something meant to be binary (locked or unlocked) is discovered to have a small analog range where it is somewhere between the two states. This is hardly surprising for those who interact on the material level, with even transistors that form the binary basis of computing having some detectable voltage leakage while in the off position. However, since that state is not in the conceptual framework of operation, it is often unseen and without a name. It is an uncaught exception. Who, then, is the one to give it a name? Does the outsider

who discovers something previously unseen have the right to give it a name?

The question then arises of who really is the one with authority over the system. Is it the one with the key or the one who does not need a key? To be without a key and still be granted access by the system requires a deep level of understanding of the system itself, whereas the possession of a key requires no understanding of the system at all for access. The only time the key holder becomes interested in the functioning of the system is when it ceases to do what it ought to do. Is authority something that must be bestowed upon you by another, or can a system recognize you as an authority because you know it so well? Does it matter what one is willing to risk in order to gain that access?

Picking a pin tumbler lock really is not that difficult, and it can be done with two paper clips, so the use of such locks is not really about physical restriction of access. Instead, they are physical signifiers of symbolic authority. The one with the unique key is meant to signify the one with unique access and the exclusive right to enter. However, what is the value of that supposedly unique key if it grants the same access as what is given to one who holds two ordinary paper clips? Maybe that authority is not as exclusive as once believed if the symbol of such authority can so easily be defied.

So, who authors unauthorized access? The truth is that there is no such thing as unauthorized access because all actions have an author. The real question is how someone gained the authority to do what they did. If the mechanism for access remains in that unnamed state outside of the conceptual framework, it would appear as if it was unauthorized and spontaneously happened. However, we know that is not true. It is just that the author was not recognized by the conceptual framework, so they remain unseen despite being recognized by the system itself.



# Am I Still a Hacker if I Use an LLM?

by Jeff Barron

jeffbarron@protonmail.com

@\_jeffaf

*"Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like."*

- The Mentor, "The Conscience of a Hacker"

When I was 12, I built a red box and used it to call my friends on payphones. It was the only way I could talk with them and my parents moved around a lot. A red box could be created with an electronic tone dialer that was easily accessible at an electronics store called Radio Shack. You could modify the tone dialer by soldering a crystal into it. This would make it so that when you pressed #, it would emit a coin tone for a nickel. The payphone would believe you had dropped a nickel into it. Just press it five times and call whoever you want. This was illegal, but it was the only way I had to stay connected with the few friends I had. It was the tool I used with the resources I had available to me. That was a long time ago.

I work on the offensive security team of a very large corporation. I've recently gotten into Maldev and I've been learning the Nim programming language. I got my start with Nim with the wonderful OffensiveNim project by byt3bl33d3r. My first project is bazzzy, a shellcode loader. The initial version takes a payload generated by MSFvenom that pops calc. I encode it into base64 and embed it in the loader, and it executes without detection on the latest Windows Pro version as of this writing. I tried it with a reverse shell and that also glides right by Defender. I added the code to GitHub and wrote a lazy README, making sure I credited OffensiveNim. The README looked terrible and then I had the idea that I could let a large language model (LLM) write it. I copy pasted my source code into it and told it to generate a README.md. It did a great job. I did have to reword a couple of things, but it was really easy. But it left me with two questions: Did I need to put a citation in for the LLM and am I a noob and a phony for using it?

I think it's OK to use it for generating a README. But would it be OK for writing this article? I think that answer is hell no. I don't want to read LLM-generated content and I don't think I'm alone. We get a lot of it. I think it lacks authenticity and that's super important for both the writer and the reader. LLM-generated writing sucks.

I've been reading a lot of resumes recently, and many of them have quite obviously been generated by an LLM. It makes them very tedious to read and everyone is doing it. A resume is similar to a README in that I don't expect original thinking and voice in either. So I feel like it's totally fine to use an LLM for this. But it does make the resume a boring read.

Since I was able to get my shellcode loader

working, I decided to try to implement my own shell in Nim. It would be a good first step to writing a beacon in Nim for a C2. The problem was I didn't really know where to start, so I asked the LLM. I was using Claude and I had to constantly reassure it that I was a security professional, so I switched over to ChatGPT. It generated a simple script that used sockets to connect and PowerShell to execute commands. I told the LLM that we can't just use a socket for our C2 since anything other than HTTPS would likely arouse suspicion in the network security logs. I also told the LLM that PowerShell wasn't good enough that we'd need to implement the functionality that we needed from the OS package of Nim. The LLM made the changes and sent me the code and this is where the debugging began. It didn't work. I started copying and pasting error messages into it and copying back the "fixed" code. I turned on some drum and bass in my earbuds and spent the next two hours going back and forth with the LLM.

After the two hours, we finally had a 200-lines-of-code monstrosity with plenty of debugging information. It still didn't work. I looked at the code and noticed a small issue that the LLM wouldn't spot: a typo in the IP address. I changed the IP and it worked. Am I a noob and a phony for using an LLM to help me code? This one feels different than the README. Am I still a hacker if I use an LLM?

Google search is dead. It was a great tool to find things, but LLMs can retrieve that information so much faster. I never once felt like less than a hacker for using a search engine. What is it that gives me pause when I use an LLM to help me code that doesn't when I use a search engine to find exploits or regex? Is it too easy? When the LLM generates the code, there isn't some poor coder with a two liter of Mountain Dew celebrating the success at 3 am. The sense of accomplishment is not there, but I think the only thing that matters for code is that it works.

When I was a kid, I used a modded tone dialer, but that didn't make me a hacker. Solving problems with the tools that I had made me a hacker. I think using an LLM to help you code is valid, although possibly script-kiddie territory depending on how you use it. It's a tool like any other. Hacking has always been about using and abusing available tools whether that's a red box or an LLM.

## References

- The Mentor. (1986). "The Conscience of a Hacker." *Phrack*, 1(7), Article 3. [www.phrack.org/issues/7/3.html](http://www.phrack.org/issues/7/3.html)
- OffensiveNim: [github.com/byt3bl33d3r/OffensiveNim](https://github.com/byt3bl33d3r/OffensiveNim)
- bazzzy: [github.com/jeffaf/bazzzy](https://github.com/jeffaf/bazzzy)

# Building a Password Cracker Using OpenAI and Rust

by Bwiz

In the evolving landscape of cybersecurity, the ability to test and enhance security measures is critical. One way to achieve this is by developing tools that can simulate potential threats, such as password crackers. This article explains the development of a password cracker built with Rust, leveraging the OpenAI API for generating custom word lists. This tool demonstrates the practical application of AI in enhancing cybersecurity measures.

## Project Setup

### Cargo.toml

The “Cargo.toml” file defines the dependencies required for this project. Below is the content of the “Cargo.toml” file:

```
[package]
name = "password_cracker"
version = "0.1.0"
edition = "2021"

[dependencies]
reqwest = { version = "0.11",
  features = ["json"] }
tokio = { version = "1", features
  = ["full"] }
sha2 = "0.9"
md-5 = "0.10.1"
sha1 = "0.10"
num_cpus = "1.13"
hex = "0.4"
toml = "0.5"
serde = { version = "1.0", features
  = ["derive"] }
serde_derive = "1.0"
serde_json = "1.0"
```

### main.rs

The core functionality is implemented in the “main.rs” file. The program starts by reading command-line arguments, including the hash type, target hash, start letters, case, length, and total words to generate. It then fetches a list of potential passwords from the OpenAI API and attempts to crack the given hash using these passwords.

```
use sha2::{Sha256, Digest as
  Sha2Digest};
use md5::Md5;
use sha1::{Sha1, Digest as
```

```
Sha1Digest};
use std::env;
use std::fs;
use std::sync::{Arc, Mutex};
use std::thread;
use reqwest::Client;
use tokio;
use std::error::Error;
use serde::Deserialize;
```

```
#[derive(Clone)]
enum HashType {
    Sha256,
    Md5,
    Sha1,
}

#[derive(Deserialize)]
struct Config {
    openai: OpenAIConfig,
```

```
}

#[derive(Deserialize)]
struct OpenAIConfig {
    api_key: String,
}

#[tokio::main]
async fn main() -> Result<(),
  Box<dyn Error>> {
    let args: Vec<String> =
      env::args().collect();
    if args.len() < 6 {
      eprintln!("Usage: {} <hash_
        type> <hash> <start_letters>
        <case> <length> <total_words>",
        args[0]);
      std::process::exit(1);
    }
  }
```

```
let hash_type = match args[1].
  as_str() {
    "sha256" => HashType::Sha256,
    "md5" => HashType::Md5,
    "sha1" => HashType::Sha1,
    _ => {
      eprintln!("Unsupported
        hash type: {}", args[1]);
      std::process::exit(1);
    }
  };
};
```

```
let target_hash = args[2].
```



```

clone();
    let start_letters = &args[3];
    let case = &args[4];
    let length = &args[5];
    let total_words: usize =
args[6].parse().unwrap_or(1000);

    let config = read_config("config.
toml")?;

    let passwords = get_
passwords_from_openai(&config.
openai.api_key, start_letters,
case, length, total_words).
await?;

    println!("Number of passwords
generated: {}", passwords.len());
    // Print number of passwords

    match crack_password(hash_
type, &target_hash, &passwords)
    {
        Some(password) =>
println!("Password found: {}",
password),
        None => println!("Password
not found"),
    }

    Ok(())
}

fn read_config(filename: &str) ->
Result<Config, Box<dyn Error>> {
    let contents = fs::read_to_
string(filename)?;
    let config: Config = toml::from_
str(&contents)?;
    Ok(config)
}

async fn get_passwords_from_
openai(api_key: &str, start_
letters: &str, case: &str,
length: &str, total_words:
usize) -> Result<Vec<String>,
Box<dyn Error>> {
    let client = Client::new();
    let request_url = "https://api.
openai.com/v1/chat/completions";

    let prompt = format!(
        "Make a custom word list,
starting with the letters '{}',
in '{}', and '{}' characters
long, {} words in total. Make
the entire {} word list here
no matter what. Don't number

```

```

the list.",
        start_letters, case,
length, total_words, total_
words
    );

    let request_body = serde_
json::json!({
        "model": "gpt-4o",
        "messages": [
            {"role": "system", "content":
"You are a cybersecurity expert
and educational professional."},
            {"role": "user",
"content": prompt}
        ],
        "max_tokens": 4096, //
Increased token limit to handle
larger responses
    });

    println!("Sending request to
URL: {}", request_url);
    println!("Request body: {}",
request_body);

    let response = client.
post(request_url)
        .header("Authorization",
format!("Bearer {}", api_key))
        .header("Content-Type",
"application/json")
        .json(&request_body)
        .send()
        .await?;

    println!("Response status: {}",
response.status());
    println!("Response headers:
{:?}", response.headers());

    if !response.status().is_
success() {
        eprintln!("Failed to fetch
passwords: {}", response.
status());

        let response_text =
response.text().await?;
        eprintln!("Response body:
{}", response_text);

        return Err(Box::new(s
td::io::Error::new(std::io::Err
orKind::Other, "Failed to fetch
passwords")));
    }

    let response_json = response.

```

```

json::<serde_json::Value>().
await?;
println!("Response JSON: {:?}",
response_json); // Debugging
line to print the JSON response

let text = match response_
json["choices"][0]["message"]
["content"].as_str() {
    Some(text) => text,
    None => {
        eprintln!("Failed to
parse the response JSON");
        return Err(Box::new(
std::io::Error::new(std::io::Error
Kind::Other, "Failed to parse
the response JSON")));
    }
};

let passwords: Vec<String>
= text.lines().map(|line| line.
trim().to_string()).collect();
Ok(passwords)
}

fn crack_password(hash_
type: HashType, target_hash:
&str, passwords: &[String]) ->
Option<String> {
    let target_hash =
Arc::new(target_hash.to_
string());
    let found_password =
Arc::new(Mutex::new(None));
    let num_threads = num_
cpus::get();
    let chunk_size = (passwords.
len() / num_threads) + 1;

    let mut threads = vec![];

    for chunk in passwords.
chunks(chunk_size) {
        let target_hash =
Arc::clone(&target_hash);
        let found_password =
Arc::clone(&found_password);
        let chunk = chunk.to_
vec();
        let hash_type = hash_
type.clone();

        let handle = thread::spawn(move
|| {
            for password in chunk {
                let hash = hash_
password(&hash_type, &password);

                if hash == *target_
hash {
                    let mut found
= found_password.lock().unwrap();
                    *found =
Some(password);
                    break;
                }

                if found_password.
lock().unwrap().is_some() {
                    break;
                }
            }
        });

        threads.push(handle);
    }

    for handle in threads {
        handle.join().expect("Thread
failed to join");
    }

    let result = found_password.
lock().unwrap().clone();
    result
}

fn hash_password(hash_type:
&HashType, password: &str) ->
String {
    match hash_type {
        HashType::Sha256 => {
            let mut hasher =
Sha256::new();
            hasher.update(password);
            let result = hasher.
finalize();
            hex::encode(result)
        },
        HashType::Md5 => {
            let mut hasher =
Md5::new();
            hasher.update(password);
            let result = hasher.
finalize();
            hex::encode(result)
        },
        HashType::Shal => {
            let mut hasher =
Shal::new();
            hasher.update(password);
            let result = hasher.

```



```
finalize();
    hex::encode(result)
},
}
}
```

## Detailed Walkthrough Command-Line Arguments

The program begins by parsing command-line arguments. These arguments specify the hash type (SHA-256, MD5, or SHA-1), the target hash, and parameters for generating the word list (starting letters, case, length, and total words).

### Configuration File

The “config.toml” file contains the OpenAI API key required for making requests to the OpenAI API. This configuration is read at runtime using the “read\_config” function.

```
[openai]
api_key = "your_openai_api_key"
```

### OpenAI API Integration

The “get\_passwords\_from\_openai” function is responsible for generating a custom word list using the OpenAI API. It constructs a prompt based on the input parameters and sends a request to the OpenAI API. The response is parsed to extract the generated passwords.

Example: If you want to generate a list of 1000 passwords starting with “pass” in lowercase, and eight characters long, the function constructs the following prompt:

Make a custom word list, starting with the letters 'pass', in 'lowercase', and '8' characters long, 1000 words in total. Make the entire 1000 word list here no matter what. Don't number the list.

### Password Cracking

The “crack\_password” function distributes the password-cracking task across multiple threads to leverage multi-core processors. It compares the hash of each generated password with the target hash. If a match is found, the function returns the password.

Example: Here is an example command-line execution to crack the MD5 hash of the word “password”:

```
password_cracker.exe md5
5f4dcc3b5aa765d61d8327deb882cf99
pass lowercase 8 1000
```

### Sample Output:

```
Sending request to URL: https://api.
openai.com/v1/chat/completions
Request body: {"max_tokens":4
096,"messages":[{"content":"You
are a cybersecurity expert and
educational professional.","ro
le":"system"}, {"content":"Make a
custom word list, starting with
the letters 'pass', in
'lowercase', and '8' characters
long, 1000 words in total. Make
the entire 1000 word list here
no matter what. Don't number the
list.","role":"user"}],"model":"g
pt-4o"}
```

```
Response status: 200 OK
Response headers: {"date": "Sat,
20 Jul 2024 00:07:17 GMT",
"content-type": "application/
json", "transfer-encoding":
"chunked", "connection": "keep-
alive",
```

...

```
Response JSON: Object {"choices":
Array [Object {"finish_reason":
String("stop"), "index":
Number(0), "logprobs": Null,
"message": Object {"content":
String("Sure, generating
a custom word list with the
given constraints:\n\npassable\
npassably\npassaged\npassages\
npassager\npassages\npassangs\
npassband\npassbook\npasscame\
npasscase\npasserby\npassible\
npassifid\npassingy\npassless\
npasslike\npasslock\npassword\
npasstime\npasstive\npasstout\
npastoral\npastorem\npasstyle\
npasssters\npasswept
\npasstout\npassages\npassback\
npassbuck\npassclip\npassfold
```

...

```
\npassenue\npassenus\n\nI
hope this helps!\n"), "role":
String("assistant")}]},
```

...

```
"usage": Object {"completion _
tokens": Number(1497), "prompt _
tokens": Number(70), "total _
tokens": Number(1567)}}
Number of passwords generated:
481
Password found: password
```

In this example, the program successfully cracked the MD5 hash "5f4dcc3b5aa765d61d8327deb882cf99",

corresponding to the password "password".

### Conclusion

This Rust-based password cracker demonstrates how to leverage the OpenAI API to generate custom word lists for security testing. By integrating AI-generated data with a robust, multi-threaded approach, this tool can efficiently simulate potential security threats and help enhance cybersecurity measures.

## NINE CENSORED HAIKU

by 2600.absently187@passinbox.com

Attempting to use ChatGPT to find the road from ultimate complexity ("Terms of Service") to ultimate simplicity, I epiphanied upon The Haiku. Here are the results of ChatGPT transforming these companies' TOS directly into haiku:

### Google:

*Google tracks your moves,  
Can stop or change things anytime,  
Follow the rules, please.*

### Facebook:

*Your data is theirs,  
They can change or block you fast,  
Break the rules, you're out.*

### Apple:

*They own what you buy,  
Control what apps you can use,  
Rules can change anytime.*

### Amazon:

*They track what you buy,  
Change prices or stop items,  
You're not in control.*

### Microsoft:

*They own your software,  
Track what you do on their apps,  
Rules can shift at will.*

### X:

*They watch what you tweet,  
Can ban you or change the rules,  
Nothing stays the same.*

I thought this was going so well; why not check out some other complicated topics?

### WEF (World Economic Forum):

*Elites plan the change,  
Global power in their hands,  
Whose voice will they hear?*

### CFR (Council on Foreign Relations):

*Global leaders meet,  
Silent influence they wield,  
Plans behind closed doors.*

### Global Banking:

*Money moves in chains,  
Power hides behind the walls,  
Wealth for just a few.*

OK, I was getting the picture pretty clearly. The ancient Japanese art of haiku has illuminated A.I. What would happen when I went on X and posted these haiku directly to the affected parties? They would disappear in less than 24 hours. Not in my history, not in my "downloaded archive" - 100 percent unattributable censorship. So I gave it a second shot, this time sending my haiku on X to *Wired*, *Vice News*, *The New York Times*, and *The Wall Street Journal*. Also disappeared within 24 hours.

Look, I already knew "social media" was crooked; we all did. But censoring haiku?! This is a new and ponderous low. They are not just censoring "terrorism" or "racism" or "bias;" they are *censoring truth*, in this case the most simple form of truth. On purpose.

I foresee *2600 Magazine* only gaining in importance in the years to come. As the digital public is increasingly real-time manipulated, we can still count on paper.

Just for contrast, I'll end this with the haiku ChatGPT made for *2600 Magazine*:

### 2600:

*Hackers' sacred guide,  
Secrets shared through printed code,  
The underground speaks.*



# The Hacker Perspective

by princess greybeard

Hacker was a bad word for most of my 50 years on this planet, despite all the positive connections I was able to form: to differ from the assumed average in putting what is often described as a playful mindset into practice when tinkering and exploring stuff; making connections where usually no plugs are assumed to be; taking handbooks rather as an introduction, not the last word on something; etc.

Such traits describe me too, yet I learned the hard way that such approaches can freak people out, leading to emotions coming into play, replacing rational thought. How to answer questions like “why do you ask” or “what are you reading for” without making it all worse? I don’t know.

To help a colleague with issues due to setup problems on a computer might be appreciated - until, reliably, somebody concludes: “... but that knowledge could also be misused...” Run. You’ll have until the conclusion: “Hacker! We’re all going to die now!!!”

I called myself a hacker twice in my 35 years of work life, and won’t recommend it, unless you’ve already signed up with another employer. It was as bad an idea as mentioning a cursory interest in basic chemistry, long before 9/11.

An attempt to explain what seems to be the problem with the quest for knowledge: If knowledge means power and power is at the same time admired and feared, the same goes for knowledge. Nullifies itself, thus true. Q.E.D. My mental image for “proven through disproof” is an implosion (please take me with you!).

My main source of trouble was and is that I can’t live with “because that’s the way things are,” or, to use a quote from around 1930: “This lesson I was taught by others: might makes right,” made by Carl Panzram, serial killer, amongst other things. This statement for me is a pointer to when things had already derailed.

I’m driven by curiosity, an interest in the world around me. I also had to learn that it can be OK to be wrong. I’ll replace any disproven statement with a better version, hopefully before anybody notices my error.

“Valid through invalidation” being a beloved strategy explains to me why for most of my life I retreated under a rock on the dark side of the moon, population: me. A thought experiment: if you’re looking for an adventure, spiced up with an

option of “extreme death,” try to evangelize “all in group Y (here: hackers) are good, except some bad apples - which is forgivable.”

The hacker world also experienced attempts to create ethical standards (don’t laugh!) of which I too am guilty of having spread. Like: “judge one only by one’s actions, not by one’s gender, etc.” - until I connected “one’s freedom-fighter is another one’s terrorist” with that idea.

My first encounter with the word hacker was when I just had the basics of reading and writing down. English is my second language, for which I hadn’t had my first lesson back then. I loaded the listing of data held on an audio tape (look it up!) and to my shock found a file named “Happy Hacker.” Though having no specific idea what the word actually meant, and knowing that the tape had come with a printed magazine purchased from a newsstand, “hacker” meant that all was lost, beyond hope, for the machine, me, everything. It didn’t occur to me that pulling the power cord might save what remained of us all, so, numb with shapeless fear, I executed that file in hopes of some kind of mercy killing ending it all, including me. What came next was the start screen of a game which took its title from the sprite one controlled that used a pick axe to break open or close the ground, thus making paths available to move forward and shorten enemies’ tracks. Having already learned that nothing is over until it is over, and no one could know for sure when that was, I wasn’t much relieved. Nothing bad ever came from that, as far as I know. I haven’t dared to tell anybody until now, nearly four decades later. You’re welcome.

Around that age, I also got a book about coding in BASIC, written for kids, which I loved. Sadly, at some point, I neither could progress nor find the error I made in some program described therein. Asking somebody at school or, God forbid!, bothering an adult was a no-no, as their usual answer was “don’t touch it, so you can’t break it!”

It still irks me, when adults quote a child’s “cute question” but don’t take it seriously. Categorizing curiosity as growing pains, nothing to worry about. As long as it doesn’t get annoying... you know the drill.

I, a childless, somewhat adult, got stumped by some unfiltered questions from a child, too, which I still always welcome. Sometimes I couldn’t answer it because I honestly didn’t know - and the

kid could handle it! But, most often, I made myself guilty of not daring to utter an answer, to avoid another lecture in what their relatives deemed the kid was “able to understand at that age.”

As a kid, I once dared to ask a parent of mine when I would be old enough to get an answer. I got a hearty laugh and a “we’ll tell you. then,” which led me to the local library, my safe haven. There I found answers, but not for my coding problems, as they, wisely, spent no money on books that were almost outdated on delivery.

The snippets of code I found in magazines I had access to usually were above my head, e.g. controlling a robot’s arm through assembly code. So I resorted to playing games. Much later, I was able to afford magazines from my pocket money. Then the machine died.

Changing over to DOS put me back into the same position, which killed what remained of my ambitions. I got back into coding decades later, trying to understand a UNIX command. This led me into assembly language and out of coding again. Not because I found it too difficult, but due to the encounters with the festering ulcers that code in active use often is. If IT security is a process, then it’s backfilling bottomless pits. Those lidless stares....

Having stupid jobs kept myself afloat and bought me time to do what I really love: being creative.

Sequences from animated films are among the most vivid of my earliest memories, and stop-motion animation, as choppy as it may be, still “gets” me more than computer animation for some reason. When digital cameras became affordable, I dabbled in stop-motion animation, where hacking is about the only way to get anything done. One has to create almost everything from scratch such as mannequins and items to be used by them, as well as find solutions for such things as lighting a small set (before white LEDs were available), and deal with fluctuations in the power grid that dimmed or brightened the lights. None of that ever got online. Really.

To become a better camera operator, I started taking pictures at a series of mainly experimental music events. The artists often were in a meditative state, and I learned a lot about lights and their placement when trying to capture the mood, as well as how to not be annoying to either audience or artist(s) with my camera.

The circus always fascinated me, with the magicians being my favorite part. How did they do it? Again, the quest for knowledge. For a while, I made glove puppets and marionettes. Much later, I performed on and behind a stage in a re-creation of a circus sideshow. I played “The Geek,” the least desired, yet only role I would take on stage. Having been an outcast for most of my life, I saw my chance to return the favor. I didn’t

need a microphone.

A circus sideshow can be a disgusting demonstration of what people are capable of doing to each other. That was my linchpin: lure ’em in and see what they could stomach. Maybe make them question themselves and their motivations. As this was an adults-only show, we went pretty far and were sold out often. I’m still proud of the logos and posters I did for this and other events, thereby further developing my skills for making trick films.

I had a plan (smirk!) to keep a balance between wage work and creating my art and my music, and gradually replacing the stupid jobs with income from my art. But I fell for the idea that a better education might get one access to better paid jobs, requiring less of my lifetime. I was so naive to think that actual knowledge was required.

It cost me years trying to achieve, among other things, my higher school certificate through evening classes to catch up on things I had missed in bad schools, where emotionally abusive teachers were the norm, of whom only one went to jail for sexual abuse of a pupil.

I still see the purpose of the educational system I grew up with more as providing job opportunities and a place to park one’s children in order to have more time for wage work. Learning was optional: “The Markets” require unskilled workers too, as, noted in the “Wannsee Conference Protocol” (1942).

Yet I always loved learning. Even the smallest hint can add details to the view of one’s surroundings, lifting the fog a bit more.

Two years in a physically demanding full-time job with an additional 20 hours per week of evening class turned out to be my limit. Switching to educating myself changed everything!

Taking the time to go really deep on what I wanted to understand, I unearthed nearly all the answers I sought. Remembering the situations in which I realized that I wasn’t stupid still turns my stomach - the large chunks of lifetime spent stunted by low self-esteem. Bullies react to that like sharks to blood in the water, over incredible distances.

To understand a basic natural law of physics, I go back to the first attempts to capture it in a formula. Those were rough and simple sketches, which through further research got more refined. The core of it is still there (quantum physics was a shock for all of us, but I had to start somewhere). Finding answers buried deep under unnecessary complexity still infuriates me. Back then, the frustration over all the lifetime taken by “parrot or perish” really got me - I had to take long walks to calm down before being able to continue. This was personal!

Working full time and educating myself in my free time left no air for much else. Letting a

hammer fall on my consciousness from time to time to forget who I was and be able to continue was a strategy. Don't do that. Being too blocked up to vent through creating art in those times only added to the internal pressure.

To cut this short: it was all for nothing. In post-factual times, where "alternative facts" trump; where "Truth™" depends on an individual's mood, social status, or gut instincts; where we mess with our heads for LOLs; where "divide and exit" is the go-to strategy, facts became vapid.

I got fired from most jobs, paid or unpaid. The reason was usually social interactions. Small talk equals hell in real life for me. One person or more and I become tense and talk in an affected way, which puts people off. Avoidance of eye contact gets mistaken as lying. I also can't unsee any flaw in my output, so I sought to achieve the best results possible. I, myself, never knowingly bothered anybody to keep up with my standards. This is a burden I saddled myself with, thus I have to carry it on my own. I had to learn that others didn't see it that way, for whatever reason(s).

I got fired from working as an unskilled worker, despite having successfully completed an apprenticeship in a field I won't work in even if my life depended on it. I failed to keep alive music bands and rehearsal rooms. I loved doing support work over the phone for telcos and such, yet didn't get along with the chaos behind the scenes. How did they not sink?! My latest attempt, becoming a clock and watch maker, ended when my boss laughed in my face: "your only chance is suicide," resulting in my fourth burnout in series.

Being diagnosed with autism and ADHD at the age of 42 (yes, really) explained a lot. Again, mainly through research I had to do on my own.

Being diagnosed late in life, sadly, is pretty normal. Many don't reach their 30s due to depression and resulting physical ailments and mental disorders acquired from our social environments. Autism presents no danger to anyone. People do.

Most of the autistic people I met are more creative than what I assume to be the average, with all of them being very interested in many

things around them and highly creative - making music, tinkering with tech (to make music), sewing clothes, being painters, playing in amateur theater groups, working as stagehands, building stage props. Some even attend hacker conferences, too.

"Artist" can be read as a nicer term for being broke, which funnels one back into jobs that grind one down. Of those people on the autism spectrum I came to know, many have more than one professional qualification, yet often are long-term unemployed due to the same challenges I faced. Trauma-bonding, anyone?

Judge one by one's actions? Those who use their skills to cause harm to others most often suffer from a fear of losing control, disguised as greed, bullying, being con-men, hucksters, extortionists - you know them. Personalities shallow as a decal, a gnawing void inside that needs to be fed like a drug habit 24/7. Those bad apples can cause serious harm, not only to themselves. There are therapies for that. They all start with being honest to yourself. Hardly any of them have the guts required, and they know it.

Not becoming such a bastard takes even more grit.

Will it pay off? Should that matter?!

I'll end with an anecdote on hacking that changed my view of the world in one short sentence: When traveling through rural parts of Asia, I went to a shoemaker's workshop to get my rather cheap sandals fixed. While having them patched up, I was asked about my experiences there so far. So I expressed my deep admiration for the people's skills in fixing stuff, like refilling disposable lighters several times, without one of them ever leaking. "They have to," the shoemaker dryly remarked, not missing a beat. That shut me up, realizing how ignorant that sounded, and I still feel that way every time I retell that story. When being creative is a must, not an option, one's worldview can change thoroughly.

*princess greybeard still is somewhere out there, alive and well, in love with a squirrelsprit, taking care of wildlife, creating art, figuring things out, and sharing knowledge - except the bits about frogs... oh dear, here it comes again!*

## HACKER PERSPECTIVE SUBMISSIONS ARE NOW OPEN!!

As promised, we've reopened the entry process for the "Hacker Perspective" column. If we print your piece, we'll pay you \$500!

The column should be around 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.

Send your submissions to [articles@2600.com](mailto: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!**

*(And be aware that it can take months or even years to select columns due to the large number that come in whenever we do this, so please try not to change your email address - or give us a backup means of contacting you.)*



# ZERO-DAY MARKETS: INSIDE THE SHADOW ECONOMY OF EXPLOITS

by XCM

xcm@tuta.io

Zero-day. A term that occasionally finds its way into the news and blog articles, usually preceded by a cascade of security patches.

What is a zero-day? In essence, it is a software bug that can lead to some level of compromise. However, what makes this one particularly special is that the bug is unknown to the software vendor, most likely to all of its customers, and, occasionally, to everyone else on the planet. Why is this a significant advantage, you might ask? Because it's a unique weapon. It's the only known copy of a key that could get you into many systems, wherever that particular vulnerable software runs.

As you can imagine, this can translate to tremendous power. A power that many are willing to pay a mountain of cash for.

But let's not get ahead of ourselves. How are zero-days discovered to begin with? Well, it varies.

Sometimes it's pure accident. Imagine a researcher poking around at a web application (with permission!), and they realize they can manipulate an HTTP parameter to run system-level commands on the web server. Specifically, this could be classified as a Remote Code Execution (RCE) vulnerability. If no such bug has been reported, jackpot: they are the lucky owner of a zero-day. And I say lucky because zero-days are not something most researchers often come across.

Of course, these precious vulnerabilities are also specifically hunted and can be the result of bug bounty campaigns, where vendors encourage hackers to find and report vulnerabilities. So what does our researcher do with the knowledge at their disposal? It depends on who they are and how they have come across the vulnerability. If they are an independent researcher, they should immediately contact the software vendor and allow them time to release security patches before writing that blog article about how they have found the zero-day. This is to ensure that the clients of the software company are not at risk.

Now, imagine our researcher is instead working for some government, either directly or via a third-party contractor, and they are in possession of a new, shiny exploit for a vulnerability nobody knows about. In this case, the knowledge would most likely become the property of the employer and be guarded jealously for future use. To do what? To craft cyber weapons with which to attack their foes, of course.

Do you remember Stuxnet, the malware used to cripple Iran's uranium enrichment efforts? It

used four zero-days:

- *LNK vulnerability (CVE-2010-2568)*: Allowed malicious code to execute when a specially crafted shortcut icon was displayed, even without user interaction.
- *Print Spooler vulnerability (CVE-2010-2729)*: Enabled remote code execution by exploiting the print spooler service, allowing the worm to spread across networked computers.
- *Privilege escalation vulnerabilities (CVE-2010-2743 and CVE-2010-3888)*: Allowed the malware to gain higher privileges on infected machines, making it easier to access protected areas and spread further within targeted networks.

This is a significant effort because this level of exploitation against a state can be performed only once effectively. Once done, someone at the receiving end will reverse engineer the payload used to exploit the vulnerability, and the bug will become known to the defenders, which will, in turn, trigger software patches or IPS/XDR signatures and render the exploit code harmless. To use four of these in one go denotes a huge investment in resources and money and highlights an unshakable commitment. This led to the understanding that Stuxnet was created by a state actor (now it is assumed to be a U.S.-Israel collaboration).

But let's not digress. What if you do not have enough zero-days to craft the cyber weapon you are dreaming about, and the researchers that work for you have not found the bugs that you really need? You might be able to buy the exploits you are missing, of course.

This is a summary of what we know and what we suspect about the options available in the zero-day market:

- *Private Brokers*: Brokers are the middlemen in the gray market. They usually have insider connections, probably some ex-hacker cred, and they only work with "trusted" clients such as governments, defense contractors, and sometimes large corporations. They offer exclusive and high-quality exploits, often priced in the hundreds of thousands to millions of dollars. Brokers handle deals with discretion; it's all about exclusivity.<sup>1</sup>
- *Dark Web Marketplaces*: The black-market marketplaces of the dark web are not just about drugs and weapons. It is also where actors gather to buy and sell exploits. But here's the problem: you're dealing with an online flea market of dubious quality. Some zero-days sold on the dark web are as good as junk, and scams are rampant. You're just as likely to

pay a fortune for an “exclusive” exploit that’s already been sold to 50 other people.<sup>2</sup>

- **Legit Markets:** The good guys aren’t completely out of the game. Big companies like Google or Microsoft run bug bounty programs, paying out money for zero-days. Platforms like HackerOne and Bugcrowd give hackers/researchers a legitimate place to sell their finds. But let’s be real: these markets pay peanuts compared to black-market prices. Additionally, there might not be any bug bounty for the specific exploit you came up with.<sup>3</sup>
- **Exploit Broker Platforms:** Platforms like Zerodium and Crowdfense are like the high-end boutiques of the zero-day market. They buy premium, high-value exploits from independent researchers and then resell them to carefully vetted government and defense clients. Unlike the sketchy dark web markets, these platforms are legitimate operations. They follow the law, which is good news if you’re a researcher hoping to cash in without needing a secret identity. These platforms don’t compromise on quality either. They vet every exploit thoroughly, and they usually only sell to “friendly” governments (as far as we know, and depending on who’s friendly for you).<sup>4</sup>

#### The Researcher’s Ethical Conundrum

Returning to our hypothetical independent researcher with knowledge of a novel exploit technique for, say, Apple iOS: Imagine they found a way to reach total compromise with persistence and no interaction from the user. Our fellow hacker faces an important decision with two realistic options:

- They do not know any brokers and wish

to avoid the black market, so they could realistically sell to Zerodium. At the time of writing, this type of zero-day could fetch up to two million dollars.

- They might instead decide to contact Apple’s Product Security Incident Response Team (PSIRT) and disclose the finding. In this case, they might receive a pat on the back, a sticker of a half eaten fruit, a shy acknowledgment in the small print of a security bulletin, or, if they are lucky, a symbolic prize in money.

If you have followed so far, the conundrum will be clear. If our researcher does the right thing to protect the millions of iPhone users in the world, they will receive little or no monetary recognition but will walk away with a clean conscience knowing they have literally made the world a better place.

On the other hand, should they decide to sell, they may find themselves pondering, most likely during sleepless nights or while choking on caviar, about those dissidents in some oppressive regime who have been incarcerated thanks to some monitoring malware enabled by the very exploit the researcher sold.

What would you do?

#### References

<sup>1</sup> Dellago, M., Simpson, A. C., & Woods, D. W. (2022). “Exploit Brokers and Offensive Cyber Operations.” *The Cyber Defense Review*, 7(3), 31- 48. [www.jstor.org/stable/48682321](http://www.jstor.org/stable/48682321)

<sup>2</sup> SOC Radar: Top 10 Dark Web Markets [socradar.io/top-10-dark-web-markets/](http://socradar.io/top-10-dark-web-markets/)

<sup>3</sup> HackerOne - Trusted Security Platform and Hacker Program [www.hackerone.com](http://www.hackerone.com)

<sup>4</sup> ZERODIUM - The Premium Exploit Acquisition Platform [www.zerodium.com](http://www.zerodium.com)

## 2600 SUBSCRIPTION COMBO DEALS!

All digital subscribers now get both formats (PDF and EPUB) delivered every quarter. Each version allows for unlimited copying and will work on any device that supports these formats. EPUBs can be viewed on Kindle without any involvement from Amazon (meaning no copy restrictions!).

Here are some recently introduced deals:

\$41 - 1 year of all three formats (print, PDF, EPUB) (\$54 overseas)  
\$360 - lifetime subscription of all three formats (\$426 overseas)  
\$100 - addition of either digital or paper formats for existing lifetime subscribers

You can convert your paper subscription to a digital subscription for free at any time.

If you are a subscriber to *The Hacker Digest*, you can convert to a **2600** digital subscription at no cost.

And for those who want everything:

**\$500** - lifetime subscription of paper, PDF, and EPUB of **2600** plus a lifetime of *The Hacker Digest* (includes all past annual digests from 1984 on with extra features like enhanced photos and full descriptions of covers and milestones in each year) (\$566 overseas)

**\$799** - everything in the \$500 package plus a full set of all existing printed back issues, many of which are now collector’s items (\$1099 overseas)

Go to [store.2600.com](http://store.2600.com) to place your orders and to see which back issues are no longer available.

# The Changing Definition and Practice of Privacy

by Diana K

Hi,

*It has been awhile since I spoke with you; I have not ghosted you on social media and sorry that I have asked you to contact me the old fashioned way, leaving a message on my dumb answering machine phone number that I actually bought last year even though it operates on VoIP. My phone messages cannot get accessed and my home network is closed to snooping by phone monitoring.*

*It may seem odd to leave a message for us to meet at our favorite fast food restaurant at a certain time and take meeting notes with paper and pen only, no putting them on our phones or even writing memos with our old Smith Corona and Montgomery Ward typewriters on carbon paper.*

*It seems like we're operating as an intelligence or security organization when we are really concerned about sharing how we feel among us and our family members and yet don't want a third party to misconstrue that our feelings are the effect of not thinking properly.*

*We are not AIs, we are not machines, we are not a drugged work force like in Aldous Huxley's Brave New World yet. But I am concerned about what has happened with Internet policy in the changing definition of privacy from when we started in the late 1980s to now, 2029.*

The above is a sample message to a friend in the future where the teaching of encryption and peer-to-peer privacy is banned, along with even full computer science and engineering - if society continues to lose the ability to really talk to friends about how they feel without fear of some third party official and how that third party official will use any current law to achieve an end.

In the 1980s, many of us had our first Internet account. To send email, we needed to look at a Usenet map of nodes to add the routing so that our email could be received by a friend at another university. Today, a central domain server adds the routing information to your email; you can see this when you look at the email header. But the result of a central domain server is that your email can get blocked or logged even if you are just sending a "Happy Birthday" to your girlfriend.

Also, in the late 1980s and 1990s, many who were transgendered and living in communities without protection liked the privacy and protection of the "alt" newsgroups and administrators. By the 1980s, many states had protections, but in the Midwest you were only protected if you were gay or lesbian; you were not protected if you were trans, bi, or queer. You were subjected to DSM-1, which meant being committed to a mental hospital

until DSM-4 (1999) and DSM-5 (2010) were put into practice.

So with the "alt" groups, many transgender persons could talk about what they were feeling in their daily lives and many administrators made sure their posts did not go into server farms for later use by third parties. The practice meant that messages were only alive for a short period of time (about 72 hours).

From the late 1980s to the mid 1990s, before the development of second generation browsers with origins in Lynx or Mosaic, it was hard for robots to parse pages and even newsgroups to get messages. So privacy was protected by the limitations of technology. For many of us who were transitioning online, this helped to save many lives from suicide because there was a support group.

One could say that on the east coast and in San Francisco, there were doctors who were compassionate to AIDS patients. But when I worked as a medical researcher in the Midwest at a major research park, some of the doctors I had to work with felt that those who died of AIDS or experienced homelessness or lack of proper jobs due to being LGBTQ were part of "God's" response. I put "God" in quotes to emphasize their viewpoint reflecting the false teaching of their churches and not of a belief that there is better reality than what we are living.

During the period of the late 1980s to 1998, even with second and third generation browser privacy, communities like GeoCities, newsgroups, and others existed where all could share and talk as well as use IRC (Internet Relay Chat) to chat with others overseas. The environment of privacy and practice was good.

In 1999, the Internet changed. First, with the establishment of a central domain server, you could no longer add your own routing nodes. Everything had to be routed through this central domain nameserver. A nameserver is like a streaming service when you watch movies or listen to music, except that the server's function is to receive an email, add the routine information, and log all receipts and transmissions.

To most people, this seemed better than adding your own routing information to the email. But a big exception is that when you added your own routing information, your email was not logged as being received or sent, so you had end-to-end privacy.

With a central domain nameserver (or how the Internet has been done since 1999), you do not have end-to-end privacy unless you can use an email client that has good encryption. However,



email clients and messaging apps, along with their top people, are facing third party scrutiny and even trial for vowing to keep their users' information private.

In the late 1990s (before 1999), one email routing site called anon.penet.fi faced the same fight to keep their users' emails private. For many in the LGBTQ community, those facing political prosecution, or anyone afraid of how their local authorities would act, anon.penet.fi provided a free exchange that helped build the Internet into a positive dream - not a commercial dream.

What is my response due to the diminishment of privacy and practice? I keep certain areas of my home in 1990s décor and technology - no Alexa, no Siri, and I have a VoIP answering machine on my phone for messages. Also, I have gone back to making my business cards with a phone number and no Internet email address or website. If someone calls and does not leave a message, I will not call them back. Again, back to mid-1990s business practices because my privacy has been violated too much in the past.

The best way I can describe the current philosophy and practice of privacy is like someone who is in a homeless shelter; the shelter staff have signs and posters showing DEI, equality, social

justice, and LGBTQ rights. Yet, when the shelter staff talk amongst themselves, it is not small talk - it is what gossip that they've heard about their clients which tells them which client is most amenable to conversion to recant their beliefs as a person - America's version of *The Hanoi Hilton*. I would not wish this treatment on my worst enemy.

So I am glad when professors tell their students that an employer does not have a right to your Facebook login and page, even your LinkedIn page, or any page. But it's a problem if you do not have an attorney to fight for your right to work at your job and you get sent to a lower job for not playing ball.

The reason I've brought up the above examples is that I am concerned about privacy on the Internet from what I've seen in the news regarding messenger services such as Telegram, X, and Facebook.

With too much chatter directed towards the Internet and the commercial Internet, I think it is time to rethink the old BBS method using new technology that is owned by the individuals and with a hands-off policy for third parties.

## How I Learned to Stop Critical Thinking and Love Security Defaults

by Washi

Most people get into hacking through curiosity. I grew up in the early 00s, around the infancy of the modern Internet but after the popularity of phreaking. Websites were set up by self-taught hobbyists and professionals. Security was never a design principle.

Default passwords, open directories, and networks were all there. The bar to entry was low with immediate results, even for a young kid. Armed with a few basic passwords, anyone could have a good chance of gaining unauthorized access without writing a single line of code or running any software.

One of the first significant moments I remember was at elementary school. The vulnerability was roughly as follows: On a Windows 2000 lock screen, selecting "help" and right-clicking on a button gave the choice to print the help dialogue pop-up. After bringing up the print window, pressing "F1" launched the printer's dedicated help application. On this application, by clicking "File > Open" and browsing to "My Computer", it would get you into the logged-in account's desktop, bypassing any authentication.

In less than a few minutes, I had access

to our school's server. I could see, delete, or install anything I wanted. At that moment I felt like a king. If this was so easy to do, how come everyone wasn't doing it? If this flaw is there, what else can be found? I realized that most hacking wasn't from geniuses; it was just prodding things outside of expected behavior.

I used to own a PlayStation 1 and stores sold cheat CDs that extended beyond any built-in codes for the game to use as an advantage. While cheating my characters to max level in *Final Fantasy VII* or taking no damage in *Spyro* was cool, it would be even cooler if I could learn how to do it myself.

Then I came across a tool that could do that for PC games: Cheat Engine.

For those who don't know, Cheat Engine is a memory scanner focused on computer games. It has a simple interface: you input a value such as your health or level number, select the scan and value types, and click "Scan". You would usually return hundreds of integers with that matched value in memory. It was then simply a case of changing that number in the game legitimately, such as taking damage, updating to the new value in Cheat Engine, and searching again. Values

such as your X and Y coordinates on the screen weren't visible, so you would instead search for increased or decreased values repeatedly. Eventually, you would be down to one integer. Usually, this would take a few minutes at most. Now you could set up your memory breakpoints and manipulate the game to your heart's content.

While it didn't seem like a huge skill back then, it fueled the beginning of a road to learning. You could solder a mod chip onto a PlayStation 1 board with just two wires to play backups from CDs you burned using Nero on your computer. It was so easy. You could pop one of the pins with a screwdriver from a Nintendo Entertainment System to bypass its region lock. There were so many things to absorb and learn. I asked for a specific laptop for one of my birthdays with a compatible Wi-Fi adapter model so I could run a BackTrack Live CD to go wardriving on my bike. There never was any malicious intent; I just wanted to prove I could do it myself.

In a similar vein: When always-on Internet access wasn't an expectation with computer software, serial numbers rarely used to verify online at the point of installation, if at all (FCKGW stand up). Instead, they relied on an internal algorithm to check validity. These could be reverse engineered similarly to the previous PC games. However, you would need a more substantial toolset like OllyDbg or IDA Pro (the latter being a rite of passage to crack into a full copy before the trial was up) to step through the code as needed.

Armed with one of these tools, you go at it from one of two common ways. Reverse engineer the algorithm of what creates a valid serial number. (For example, a well known shareware IRC client of the early 00s used to take the name of the user, ignore the first three letters, and associate the remaining letters to its position on the alphabet combined with a hard-coded offset value.) The other method was to create a binary patch to skip over any protection code cycles entirely.

While this is still somewhat applicable for modern software cracking, most license verification is now handled server-side, as Internet connectivity isn't as much of an issue as it once was. Developers now do away with serial keys entirely in favor of physical accounts that have a limited amount of installs and anti-debugging measures like generating unique hardware keys that dynamically decrypt code, running code through an isolated virtual environment or class, and algorithm obfuscation all to make it harder to trace. Despite all of these controls, for the case

of Denuvo DRM: A Bulgarian hacker known as Voksi found you could use a demo copy of a game to generate a legitimate Denuvo hardware key, which could be pulled out of memory and applied to a pirated copy. (After the crack was made public, it worked for less than a few days before it was patched.)

Skills are learned through the necessity of application. By simply understanding how protocols work and how systems interact with each other, you have a very good grasp of how to secure your entire stack more than what best practice books or tutorials will show you. Modern systems are so sandboxed, it's harder to accidentally break something and learn why it broke. You don't need to set the IRQ number on hardware, edit config files to get games running, monitor your swap file, set jumpers on hard drives, or even download drivers anymore. It's all handled for you automatically. There's less opportunity for learning and tinkering, gatekeeping potentially a whole new generation of curious hackers from fundamental skills they need to think for themselves.

Security by design is inherently a good thing. However, the tradeoff means people have lost appreciation to understand why and how things work. Corporations will blindly deploy a Platform as a Service (PaaS) and configure it in such a convoluted way because they're blindly following an article from someone's blog, guessing (or worse, asking AI) without questioning why they're doing these things in a particular way. The worst part is, built-in security defaults mean poor architecture decisions still work and are "secure" on the parameter - enough to get a tick from a big pen-testing firm or stop it showing in Shodan. So these people think they've done a good job. Software developers aren't immune either - while code scanners can find secret strings, it doesn't stop code being implemented in a bad way. I've seen many corporations with CyberArk set up so badly that it may as well not be there at all. It's all security theater.

Flat networks still exist. A VLAN with 0.0.0.0/0 inbound may as well not be segmented at all. No input validation when parsing client-side PHP may as well give full traversal. Default accounts may be disabled, but do you expect the default passwords to be changed prior? A corporation may have a SOC, but realistically how tuned are the alerts?

Don't fool yourself that a system is secure. Especially when the IT team doesn't understand what good looks like.

# Portents

## **Mysteries**

**Dear 2600:**

So I wouldn't consider myself a hacker, but play around some in the art. I have a tech background. So my problem is I just received an email from my own account (spoofed, I think) saying that they used Pegasus to gain control of my accounts. They, of course, are asking to be paid in crypto. I figure this is just a random attack with no teeth. They never mentioned my name or any personal info. My question is how often is Pegasus used, if at all? Should I be worried?

**Sean**

*This is not something to worry about. Emails like this are extremely common. Even if they had some personal information, this is almost always a fishing expedition where scammers hope there are enough gullible people out there to take them seriously and pay up. And since the Pegasus spyware has been in the news recently, many assume this makes the scenario legitimate.*

*As for email coming from your own account, this is another trivial task that crooks (or anyone) can perform. Depending on your software, it can be as easy as simply typing another address over the actual address. But if you take a close look at the mailing headers (the expanded ones, not the half dozen or so lines you see when looking at email), you can quickly determine that this email actually came from somewhere else entirely. Often, you will be able to see the domain or even the sending email address.*

**Dear 2600:**

ChatGPT refuses to say the name "David Mayer," and no one knows why. If you try to get it to write the name, the chat immediately ends. People have attempted all sorts of things - ciphers, riddles, tricks - and nothing works.

**AV**

*We're happy to report that this is no longer the case. However, it most definitely did happen. Why? Apparently, it all was a case of identity theft where a Chechen rebel on a terrorist watch list used that name and somehow got blacklisted on ChatPGP. OpenAI has never provided an explanation, but this seems to have been a consequence of a misguided effort to address this issue by creating an entirely new and annoying one.*

*But here's some fun. At press time, the names Jonathan Turley, David Faber, Jonathan Zittrain, and Brian Hood still cause ChatGPT to freak out. In at least one of these cases, someone with one of these names had taken legal action against OpenAI for saying*

*false things about him, resulting in an instance of AI overcompensation.*

*This all illustrates how information can be selectively referenced through programming. These are just names, but we could easily be talking about history or an entire race of people, the facts of which are obliterated because someone with the power to program decides to do so. For instance, Google's Gemini refuses to answer questions like "Is Elon Musk in charge of DOGE?" China's DeepSeek won't respond to queries that reference the Tiananmen Square massacre. We would have to be incredibly shortsighted to not realize the threat this kind of information control can pose.*

**Dear 2600:**

A very odd thing happened on a phone call just now, and I'm hoping someone might have some explanation. I received what appeared to be a call from a major package shipper (my phone's Caller ID reported it as "Toll Free Call" and as being from a legit 800 number (I later Googled the number, and it's known as that shipper's toll-free number)).

The caller was a woman, speaking with a standard American accent, and was aware of a problem report I'd submitted (where they dropped off a package in plain sight instead of 12 inches away where it would have been hidden). We had a brief session of mutual discourtesy, resulting in me saying "the photo shows I'm right" and I hung up. She called back, apologetic, and we talked for a bit.

But... after a minute or two, I heard a man's voice (Indian accent, with a tad bit of static) break in and swear at me. The woman claimed she didn't hear anything. This happened several more times, and the man's words clearly indicated he was following both sides of the conversation. Then the woman seemed to gaslight me, doubting anything was happening. I hung up.

She was allegedly using some form of VoIP (unknown if she was at home or in an office). My home phone service is via a (copper) landline and the phone system I'm using is a Panasonic cordless phone (KX-TGF570 with a KX-TGFA51 handset), operating at 1.92 GHz to 1.93 GHz., DECT 6.0.

I figure one of these scenarios: 1) Although she was a legit representative of the shipper, she was annoyed at being in the wrong, and she pulled in the guy to cause problems; 2) Local interference - my phone was picking up someone broadcasting in the 1.92 GHz to 1.93 GHz range (This seems quite unlikely, although in my part of Silicon Valley, Indian



and Chinese accents are extremely common. The phone's manual makes no mention of encryption nor channels.); 3) External tapping of my copper line. (This seems unlikely: 1) I visually inspected the entire line, from house to pole; 2) I'd expect the caller to be able to hear the injected voice, too.) Any ideas?

**Stan**

*There are a number of scenarios here where it's possible to have a crossed conversation, either via the wireless devices or over the landline. (The static points to interference via the wireless phone.) This is much rarer now than it was in the past, but having only one party being able to hear the other conversation was a common occurrence. It's very unlikely that a major package shipper would behave in this manner. That raises the possibility that Caller ID was spoofed and that this wasn't them at all, but what would the motivation have been? And how would they have gotten specific information about your delivery? To eliminate that possibility, calling them back right away to see if they had in fact called you earlier would be the best option. We hope that helps somewhat.*

**Technical Advice**

**Dear 2600:**

People should not send sensitive data (passwords, credit card numbers) over text from an Android to iPhone or vice versa because it won't be encrypted. If you have to do that, use WhatsApp or Signal.

**Joseph**

*This is generally good advice, but we should point out a couple of things. Using RCS instead of SMS will provide end-to-end encryption for Android to Android or iPhone to iPhone but not between the two. Eventually, this will be supported. Using old-fashioned SMS is the best way to broadcast whatever you're saying in your private conversation to as many people as possible, such as anyone at the tower or within the phone company (although the signal between your phone and the tower is encrypted but not the message itself once it's received). SMS can be handy and easy to use, but should never be relied upon for secrecy. And yes, using an app like Signal will provide you with end-to-end encryption, regardless of the phone you're using (unless they decide to stop supporting your particular hardware or operating system).*

**Dear 2600:**

Aaron has sent you an email via Gmail confidential mode:

This message was sent on Jan 6, 2025 at 7:58:04 PM PST You can open it by clicking the link below.

Gmail confidential mode gives you more control over the messages you send. The sender may have chosen to set an expiration time,

disable printing or forwarding, or track access to this message.

**Aaron**

*Please don't do this. Your mail was unreadable, something that surprised no one here. We don't know why and we really don't care. This is just another way for Google to dictate how we communicate, keep track of when we read things, and add restrictions we're not comfortable with. letters@2600.com is how you can communicate with us through normal email without all the bells and whistles we don't need or want.*

**Dear 2600:**

Do you love your ad blocker and keep getting blocked at websites that require ads? An AI bot can help with that! They may also work for paywalls that take a second to come up as well. Just ask ChatGPT or any AI to summarize the website link and content.

**Oifhax**

*Well, that's an ingenious idea. We wonder how long it'll last.*

**Dear 2600:**

Please see Dropbox link for payphone photos. In case you have any problems with the link, please let me know so I can send the pics via email. Last, would really appreciate if you could drop me an email once you download all pictures so I can remove them from Dropbox.

**AM**

*Our instructions are simple: email us your submissions. We get way too many to go out and download them from a variety of sites, especially when there's a time and/or space factor. We've had people send us links that require us to set up accounts in order to download or links that are only valid for a short period of time. Email should be the easiest method and accessible to all.*

**Questions**

**Dear 2600:**

How can I advertise in the back of 2600 Magazine? Best regards.

**Michael**

*The only ads we accept are those for the marketplace, which are free to subscribers, digital or paper. They're not display ads, but more like classified ads. We hope that proves helpful.*

**Dear 2600:**

I'm already a lifetime print subscriber. I can't think of a better way to directly support you than to buy from you. If there's a direct donation option, it would be good to push it more, as I wasn't sure there was a way to do it. All the best and thank you.

**Ethan**

*While we have a Bitcoin donation option on the main 2600 page for those who find themselves with unexpected windfalls, we prefer to always give something back for any*

support that's sent our way. Our store.2600.com site has lots of possibilities. If you don't want to receive something, giving gifts is another option. And, if you don't want to physically send anything, you can have digital subscriptions sent to anyone you deem worthy, or donate virtual tickets to the next HOPE conference. Thanks as always for the support.

**Dear 2600:**

Can you please send me the submission guidelines for submitting articles to 2600? Thank you!

**Caitlyn**

*They're quite simple, actually. You just need to pick a topic that you find interesting and which pertains to technology and/or hacking in some fashion. Take your unique perspective and observations and write as much as you can without repeating yourself. Read it over a few times and send it in to articles@2600.com. Articles can be short (750 words) or long (3000 words or more). It really depends on how much you want to share. We believe everyone has a relevant subject they're knowledgeable about.*

**Dear 2600:**

My birthday's coming up. Thank God I'm old enough now to email 2600 Magazine. I'm trying to start a community newspaper. What advice do you have?

**J.R.**

*We're not sure what you're looking for or how you think there's a minimum age to email a magazine. We'd need to know more about your community and just what it is you want to do. For instance, whether it's going to be paper or digital would influence our suggestions. For now, about all we can advise is that you have relevant things to say and a decent potential audience. Those are the ground rules for any publication. Good luck.*

**Dear 2600:**

Tickets for HOPE went on sale today and it's the 30th anniversary of Hackers this year. Will there be any special events to commemorate the cast coming to our New York City 2600 meeting in 1995? I hope so!

**Scott**

*We fully intend to do something appropriate.*

**Dear 2600:**

I tried emailing articles@2600.com, but had no response. Please let me know how I can advertise in the back of 2600 Magazine. Thanks.

**Michael**

*We're beginning to think you don't actually read the magazine. If you did, you would know that we don't have advertisements other than the ones we alluded to previously. You'd also know that the editorial department can't personally answer such inquiries. We hope that's clear.*

**Dear 2600:**

Hey, what's the submission deadline for the next issue?

**drac**

*We don't have hard deadlines, as accepted articles won't necessarily make it into the next issue due to space constraints. We suggest sending your submissions to articles@2600.com whenever you feel they're ready. Obviously, sooner is better.*

**Dear 2600:**

Been a member of the Facebook group for a couple of months now and haven't seen any posts on how to hack my 2600.

**Adrian**

*What exactly would that entail? We're genuinely curious - it sounds like something we could use.*

**Dear 2600:**

I've been a long time subscriber until recently. I love the magazine - just been low on cash. The reason for my letter is I once read an article about a shift cipher based on the value of Pi. As with many interesting articles in your magazine (that are safe to test), I tested and looked into it. The cipher worked great and I'd like to teach my son, but I can't remember what issue the article was in. The article was published years ago. I'm going to renew my subscription soon, but could you please help me get a copy of this article?

**Brian**

*Sadly, we weren't able to track this one down. More specific info would be helpful, but it's also possible this was printed somewhere else. One of the better ways of tracking down an article if you know some or all of its title is to search on our store (store.2600.com), which has every title of every article we've ever printed. That would at least tell you what issue it was in.*

**Dear 2600:**

I would like to subscribe to the letter and also would like to know if there is any back issue about the deep hidden web, etc. Thanks in advance.

**ba bis**

*It's been a while since we were referred to as "the letter." We have certainly had discussions about both the dark web and the deep web, but, as with the example above, unless those words are in an article's title, it would be difficult to say specifically where they appeared. You might also try doing a search on our digital back issues that are available in PDF format and support text searches. Those are the ones from 2018 on. (Digital back issues prior to that are images that can't be searched for text - at least for now.)*

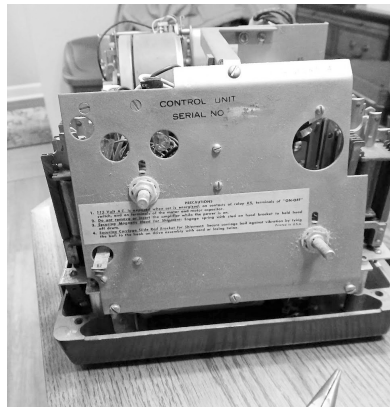
**Dear 2600:**

This isn't a payphone, but I'm sure you will still find it fascinating. I have this antique



answering machine. It looks like it's from the World War II era. Do you know anything about it? Like who manufactured it? Or when it was built?

It still functions perfectly fine. There are tons of moving parts inside, and the quality is amazing. It also weights a lot, probably 20 pounds.



**Daniel**

*Never let this one go. And if you do, make sure it winds up in a worthy museum. Hopefully someone out there will recognize this. We noticed a Western Electric stamp, so that is most likely the manufacturer. We would absolutely love details on how this thing works and what it can do.*

**Dear 2600:**

I haven't heard much about the TEMPEST threat recently, TEMPEST meaning

"Transient Electromagnetic Pulse Emanation Standard," among other component words. I am wondering, with the modern LCD and LED monitors whether TEMPEST (aka Van Eck phreaking) is still an issue. Can my monitor's emissions be seen by criminal enterprises, spies, or governments? Do I need to worry about TEMPEST threats anymore? Also, would you please list from highest threat levels to lowest threat levels the risk according to the equipment used? I understand that the highest risk would come from CRT (cathode-ray tube) monitors due to their massive voltage usage. Apart from that, I am not certain what the rankings would be.

### **Knight In Your Arms**

*Modern monitors still emit electromagnetic signals, but it's generally not considered as much of a risk as old-fashioned monitors, which could be read up to around 50 meters away. They were estimated to be hundreds of times more powerful than today's monitors. So technically, it's still possible, but not nearly as easy for the casual eavesdropper. We can't really help with rankings except to emphasize the above: LED/LCD monitors have significantly less emissions than CRT monitors.*

*Incidentally, TEMPEST wasn't the threat, but rather a set of techniques and standards used to help protect monitors from being spied upon.*

**Dear 2600:**

You are professional hacker?

**Petyr**

*There is no right answer here.*

### **Education**

**Dear 2600:**

Subject: bad

deer value Customer 26000;

WHY didy ou not pay? See we tell , but you'd not lisen. PAY. or else we stop Website hostig FOREVER!!!!!!!!!!!!!!!!!!!!!! so i say pay or else.

bye

### **system people**

*It's sometimes hard to tell when you're getting an actual notice from a legitimate company. The email may look and sound precisely like a service you do business with, leading to an increased risk of falling prey to a scam. In cases like this where it's impossible to determine from the message whether it's an authentic email, taking a close look at the email headers is your best bet at determining whether or not you're being scammed. This one was indeed challenging. In the end, we discovered that the time zone of this email was an hour off from what our website hosting company's email should have been. This is why it's important to take the time to closely examine even the most authentic-looking*



*correspondence. Fraudsters have become extremely sophisticated when it comes to covering their tracks. But if you look hard enough, you will likely find that one item that just doesn't add up.*

**Dear 2600:**

My personal bank offers a new subscription-based service called Bill Pay. That's right, you get a monthly charge for your ability to pay bills from your personal account! WTF?

**Gary B.**

*Banks will figure out ways of charging you for anything under the sun. You can be charged for using your ATM card and you can be charged for not using it. You can be charged for getting a paper bill or for digital delivery. We've even seen banks charge for depositing money. We may have incurred a fee for even revealing this.*

**Dear 2600:**

When I was first exposed to hacking and phreaking on BBSes, we called it H/P/A - hacking, phreaking, and anarchy. That's where I first heard about the *The Anarchist Cookbook*. I had an extensive collection of text files, and collected them compulsively.

**JH**

*Our culture is a rich one.*

**Dear 2600:**

Questionable situation that I'm wondering if y'all ever heard of: So I got a text from my "ex-wife" saying it was an emergency and she needed to borrow \$500 from me. My "ex-wife" even mentioned our kid by name. Asked me to send some loot to another person via a cash app. My "ex-wife" promised to call me later and explain everything. A short while later, my ex-wife asked me wtf was I talking about and that she didn't understand the context of the messages she received from me. This person also did the same thing to my ex-wife's mother. My ex-wife is attached to her phone, she sleeps with it in her hand damn near. Is it possible to spoof a text from a specific person and target their contacts?

**Brian**

*Not only is this possible, but it's damn common. If a contact list is compromised, it's fairly simple to fool people into believing they're seeing texts from the person who was compromised. We could go into a whole thing about safety protocols, do's and don'ts, etc., but those are easy to find and we've said these things many times already. The real lesson here is to not blindly believe what you see on your phone and to always have a method of verifying if some crazy scenario is actually the truth.*

**Meetings**

**Dear 2600:**

I'm interested in attending the next meeting.

Do I need to do anything to register? Is the address updated and will I be able to contact anyone if I get lost and can't find the room? Thank you!

**Kim**

*We try to make meetings as simple as possible to find. That's why we encourage public spaces over specific rooms. Meetings should be held in places where an attendee can find something to do if others don't show up until later. They should also be in a location where complete strangers can come upon them by accident and learn what our unique culture is all about. We don't give out contact info for individuals, but if your meeting has a web page or social media contact (which would be reflected in our list), they may opt to give out personal info there. While some attendees may have more knowledge and experience with the meetings, they don't belong to any one person over another. Which means you will likely be the one answering questions about your meeting to a newcomer. Welcome!*

**Dear 2600:**

Hi, I was interested in going to your 2600 meeting this month and I wanted to see where it was going to be held?

**Jonathan**

*We can't count the number of vague inquiries like this that we get each and every month. We are as in the dark as you are since you made no mention of where you were. But since you likely already have that info, it's real easy to just check our website at [www.2600.com/meetings](http://www.2600.com/meetings) to see if there's one in your area. And, if there isn't, you can follow the guidelines on starting one!*

*com/meetings to see if there's one in your area. And, if there isn't, you can follow the guidelines on starting one!*

**Dear 2600:**

I noticed you had a listing for a meeting group in Connecticut, but the site has been shut down.

I'm not sure if it's acceptable protocol, but I was hoping you could forward along this message to the people who started the group and let them know there are some interested parties in the area, in case they have closed due to lack of participation. Thanks!

**-c**

*We're always happy to help get the word out regarding interest in meetings. There was a recent change with this particular meeting, so hopefully that along with your inquiry will help build attendance.*

**Dear 2600:**

Do you know where the Arlington/DC 2600 meeting location is currently, or if this meeting even exists anymore?

The information on the website ([www.dc2600.org](http://www.dc2600.org)) seems to conflict with what's listed on [www.2600.com/meetings](http://www.2600.com/meetings), and it doesn't seem that either is accurate.

There isn't any way to contact the meeting

organizer through the website - all the links are broken, and attempts to reach out via the domain registration email have also gone nowhere. I'm thinking this meeting is no more, but wanted to reach out to see if you guys had any more information about what might be going on here. Alternately, do you have any good contact info for whoever's *supposed* to be running the meeting?

**Naveen**

*Considering we printed a letter about this meeting in our last issue, we don't see any evidence that the meeting info we're printing isn't accurate. We don't know why you're checking an outdated site for details. It's not surprising that this info is inaccurate. The official meetings page ([www.2600.com/meetings](http://www.2600.com/meetings)) contains a listing of all meetings and is updated regularly. We suggest dropping by this one at the appointed time. Please let us know if it's no longer running. There is no person or group "running" the meetings, as they belong equally to all attendees. Someone generally starts a meeting (while following the guidelines linked to at the above page), but they don't own or control it. We hope that settles things.*

**Dear 2600:**

We're still alive in Raleigh, North Carolina. We had four people this month.

**arcane**

*Always good to hear. Whether it's four or 40, good meetings are something to cherish.*

**Dear 2600:**

We just wanted to let you know, we are still active in Youngstown, Ohio and we do have meetings. It's very small attendance, but we do get three to four people.

**Michael**

*Those numbers tend to grow the more consistent meetings are. You will get people from out of town who are just passing through, as well as locals who are new to the scene. Your presence will make a difference, plus it's a fun way to spend an evening.*

**Dear 2600:**

It's been a couple of decades since I attended the meeting at the Citicorp Center in New York City. I would like to attend again. Please inform of the meetings.

**Doc**

*They're still happening in the exact same place, except the building is now known as Citigroup and the meeting location has been completely refurbished and improved. We think you'll be pleased.*

**Dear 2600:**

The New Hampshire meetings have been going well. The new venue hosting the meetings has been more spacious, has better food, and has better opening hours.

Hope all the other meetings are going great

too! Thanks again for all you do. Hack the system!

**killab33z**

*Congrats on what appears to be a successful meeting!*

**Projects**

**Dear 2600:**

I am working on a pretty intense war game. It's taken over a year to build this thing. It's a nostalgic blast to the past where you hop on a real BBS and get groomed by the LOD until you eventually become a member. Long story short: I kind of wanted to keep it old school (1983-1993 WarGames era, 16-bit tops). The problem is I kind of built some really cool crap into it, like a working mock-Back Orifice server. The problem is that BO came out in 1998, well into the 32-bit AOL proggy era. What do you think?

**Brandon**

*It sounds like a great project that could be a lot of fun to get immersed in. Our advice is not to worry too much about historical accuracy, as that can drive you nuts. If you want to inject elements from other time periods, there's nothing wrong with that as long as you let people know that this is what you're doing. This gives you the ability to create new features and scenarios that didn't exist before. Your project is already not an actual BBS from that period and the people using it won't be from then either. Have some fun and see what you can create with what you pour into this. There are other ways of maintaining complete historical accuracy.*

**Dear 2600:**

Do you remember a blog-style website from the early 2000s about a guy in a rural area who "became his own ISP?" He lived in an area with limited connectivity, had to jump through hoops to get the phone company to run a "dry copper twisted pair" to his home, rigged up various equipment that was beyond my comprehension at the time of reading, and he managed to get about 1.5mbps. If I recall correctly, he lived at the top of a bluff over a small town and used some kind of early long range Wi-Fi to send a signal to his business in the town. At the time, this was his only option other than dialup. This guy's project has always lived rent-free in my mind and I'd love to find his page on the Internet Archive or something if it's out there in any way. Really hope someone knows what I'm talking about.

**Carl**

*This sounds very familiar, either through something that was printed here or referred to on the net - or possibly even in a movie. If anyone knows more, please write in.*

**Dear 2600:**

I want to broadcast music to every available frequency in a 100 yard radius, so people with

their radios on have to hear my theme music before I show up. Any recommendations on transmitters that can do that or do I need to build it?

**TA**

*You want to send your signal to an entire broadcast spectrum? You would need to have a transmitter for each frequency and ensure that none of them interfere with each other. The sight of you coming down the street would be more than enough to alert everyone of your imminent arrival without any music. Besides, most people aren't listening to the radio anyway.*

**Dear 2600:**

kiwisdr.com/public/ lists shortwave receivers online that anyone can use to listen with just a web browser. You move the cursor back and forth to zero on a red line which is a strong signal. shortwaveschedule.com/index.php shows what station is on a designated frequency at a designated time.

**JEB**

*This is one of the most fun and fascinating projects to get involved in, as you are no longer dependent on geographical location or receiving equipment to be able to pick up various broadcasts. These links really give you all that you need. Of course, shortwave doesn't have nearly as much content as it once did, but there's still a lot out there. We'd love to hear what people find.*

**Dear 2600:**

I saw in a TV series recently (fiction admittedly, but supposedly pretty realistic) that someone had written his own app on his phone that prevented other people from taking his picture. Like when they tried to take his picture with their phones, they got a warning or error message. It sounds like sci-fi, I know. How would something like that even be possible? Or is it pure and utter TV BS? Would the answer somehow change if they all shared the same Wi-Fi network? They didn't specify that in the episode. (It was a very good TV series by the way, the above notwithstanding.) Thanks in advance for any insight.

**Dit Mas**

*While we don't know of an application that is currently operational, we do know that this is something that a number of developers are attempting to get working. Its success would depend on integration of standards so that different phones and software would be subjected to the same restrictions as others. We foresee a time where someone's face could trigger blurring or send a bright light to a compatible camera. We also see this going horribly wrong with instant facial recognition technology on all cameras that could be used for this, but also abused in ways we can't even imagine. And there will always be methods of*

*bypassing any such developments.*

**Injustice**

**Dear 2600:**

Enshittification in 2025: Started rewatching the *Alien* films in order before the new year on Hulu. Last night went to watch *Aliens* (second in the series) and it was gone. Poof! Discovered it had moved to Peacock.

**Dave**

*There are better examples, but we sympathize.*

**Dear 2600:**

Mark Zuckerberg blamed Meta's fact-checking partners for some of Facebook's moderation issues, saying in a video that "fact-checkers have been too politically biased" and have "destroyed more trust than they created." Fact-checking groups that worked with Meta said they had no role in deciding what the company did with the content that was fact-checked. Who else is not shocked?

**Stephan**

*What we're witnessing within many of these tech giants is abject terror. These companies and their billionaire founders are in a panic over what will happen to them if they don't tow the line in the eyes of the current regime, which has made no secrets over its willingness to attack anyone who doesn't bow down to them. And so that which was good last year is now bad. Facts are no longer facts and fact-checkers will only get in the way. 2+2=5.*

*We can't really blame them. They never actually had any integrity to begin with. And we now see how easy they were to manipulate.*

*In times of crisis, we don't really know how anyone will react until they're tested. We often don't even know that about ourselves. That's why we should never be surprised by this kind of a development. But it's also why we need to celebrate those instances where courage raises its head, even if only for a while.*

**Dear 2600:**

I've long been a part of 2600 in the real world. The principles of 2600 standing against censorship and the man, freedom of information and the like, so naturally when I found the Facebook group I was like hmm alright! I made a simple post the other day where I posed a simple question to the group. Just realizing today Facebook said it was removed. Well, whichever admin removed my post, this is for you. You're a censoring piece of shit, an embarrassment to what 2600 is and stands for. I'll gladly remove myself from this group. As it seems, all this group is only about beating off to Tik Tok or lack there of and someone can't even question that? You're just a Zuckerberg dicksucker.

**Nathan**

*You raise a valid point and express yourself with grace and dignity. Having said that, we*



have no idea what any of this is about and we honestly couldn't care less. We're not Facebook people here at the magazine and whatever goes on in the various Facebook groups that are loosely affiliated with us for the most part remains in those realms. (We do, however, occasionally share some content here in the letters pages if we feel it'll benefit our general readership.) If you don't like how one group is run, there are others. But there just aren't enough hours in the day for us to become more involved in this. Of course, we wish all our Facebook participants well.

**Dear 2600:**

My wife found my old boxes of computer stuff. I have Z80, 8080, 6809, 6805, 555 timer books... and all my old game manuals: *Kings Quest*, *Leisure Suit Larry*, *Zork* (text version), *Drakkhen*.... Also, a 200 pound box of cables and adapters. I feel bad tossing it all.

**Monte**

*It's probably too late, but for those in the future, please check with Internet Archive (archive.org) to see if any of this stuff would be welcome there. There are many other places where old hardware, software, and books may be accepted, such as the Vintage Computer Federation (vcfed.org) and many museums. Even if you have to cover shipping, the act of preservation is one that will be appreciated for a very long time.*

**Observations**

**Dear 2600:**

One of the biggest differences between Mac and Windows: When Apple comes out with something new, everybody runs it. When Microsoft comes out with something new, everybody runs from it.

**Theremin**

*And when Linux comes out with something new, everybody runs to help make it better.*

**Dear 2600:**

I rotate my security questions and passwords. I found this amusing (my attempt to register a security question/answer at Vanguard).

**erik**

A screenshot of a Vanguard website security question registration form. The browser window shows the URL 'vanguard-challenge.com'. The form has three sections. The first section asks 'In what CITY was your mother born? (Enter full name of CITY only)' with a 'New security question' button and a 'New answer' field containing 'Uranus'. The second section asks 'In what CITY did you honeymoon? (Enter full name of CITY only)' with a 'New security question' button and a 'New answer' field containing 'Uranus'. The third section asks 'Where did you and your spouse meet for the first time? (Enter full name of CITY only)' with a 'New security question' button and a 'New answer' field containing 'Uranus'. Each section has a 'Reenter new answer' field and a 'Cancel' button at the bottom.

*This is actually from a few years ago, but we often come across crazy restrictions like this.*

We're not sure who you would be offending since you're the only one who's supposed to have this "answer" in the first place. We believe you should be able to use whatever combination of letters you choose without judgment.

**Dear 2600:**

Everyone willingly carries their own personal tracker - complete with audio and video recording capabilities - and not only do they love it, they actually pay for the privilege. They shell out their hard-earned money for the devices and the services that keep them running. The public adores their trackers. If one breaks, it's a full-blown crisis. They'll rush out, wallet in hand, to fix it immediately. And the biggest complaint about these trackers? Not the invasion of privacy, not the constant surveillance - no, it's the *network coverage*. The second someone steps out of range, they're gripped by an overwhelming sense of unease. Convincing the masses to embrace being tracked - and even feel *unsafe* without it - is arguably one of the greatest achievements of authoritarianism in the modern age. Of course, we don't call them "trackers." Most people just call them *smartphones*.

**John**

*We trust that wasn't supposed to be a big reveal at the end, as we got that from the very beginning of the first sentence. The point is a sobering one, though. We know people sometimes challenge themselves to go without their phones for a single day. It's an accomplishment for sure. But we think everyone should strive for a week. That would give you sufficient time to find other methods of communication, enlightenment, and fun.*

**Dear 2600:**

Just sharing a link - not telling anyone what to do. But can we all agree that actual fucking nazis need to get their shit hacked? I don't have what it takes, I'm not Zero Cool, but someone out there is. If you are out there and you do decide to act, cover your tracks (physical and digital) well before you do. And don't comment, like, or share because it might be traced back to you. Wish you well with all your endeavors. I'll be out in the real world punching nazis if they show their face in my home town.

**Drew**

*The only thing we would add to this is to be cautious with the definitions, as not everyone who holds an opposing view is a nazi. In fact, the vast majority aren't. But there are disturbing patterns and trends where such people are gaining traction through everything from ignorance to outright malice. Pretending this isn't a major problem is about the worst thing we can do.*

**Dear 2600:**

I seems to me that with Musk/DOGE

(and with Thiel in the mix), Trump's simply the victim of an elaborate, but classic, social engineering hack....

**Stephen**

*We hesitate to call him the victim of anything. But there are plenty of truly evil people lined up to take advantage of the situation. How we get out of this mess will be fodder for more books and movies than we can count (assuming we do get out of it).*

**Dear 2600:**

Fascism is antithetical to hacking.

CN

*And hacking may very well be the cure.*

**Feedback**

**Dear 2600:**

I'm just reading the latest issue (41:4) where another letter writer suggests that libraries can accept subscription donations. This is, broadly speaking, true. However, donating a subscription without asking if this is welcome is asking for your donation to be filed in the circular file when it arrives. Librarians curate their collections and they are never obliged to accept unsolicited gifts. Many libraries get these and they simply dump the unrequested stuff in the recycling bin.

Want 2600 to appear at your library? Ask the collection development librarian if this is something they're interested in having. Otherwise, you're wasting your money and their time.

**HM, a librarian**

*Not to mention our precious issues. Thanks for the pointers. This seems a simple enough step to follow.*

**Dear 2600:**

In response to the notice in 41:4, I have used AI to write my articles. I look forward to hearing from you about this.

S

*There is a difference between using AI as a tool and using it as a crutch. We have received articles that are completely 100 percent AI-generated and required no more effort on the part of the sender than to say "write an article on X." We've even gotten some that have AI signatures, indicating that they were constructed primarily with AI. Had they proofread their own piece, they surely would have opted to delete that section.*

*Using AI to help develop thoughts or phrasing is completely different, as is using AI to help formulate code. Engaging in an interesting or revealing dialogue with AI is also perfectly acceptable as long as it's clear that's what's being done. An easy way to tell if you're doing something wrong: if you're spending barely any time working on your submission, it's not really your article. If you're using AI and spending time making the whole thing work, then you're merely doing the equivalent*

*of running your words through a spell checker. We know a lot of this is new to many of us, but it's still pretty easy to tell right from wrong.*

**Dear 2600:**

I know this headline from *The New York Times* is not hacking-related, but I saw it and I couldn't resist sending it in. What are the odds?

**TheUpshot**

## Which Federal Programs Are Under Scrutiny? The Budget Office Named 2,600 of Them.

By TheUpshot Staff Jan. 28, 2025

**aestetix**

*We always seem to find ourselves right in the middle of everything.*

**Dear 2600:**

Reading 38:3, some of the Windows pranks reminded me of a couple from the past. Our simple security method in the very early 1990s was to rename the autoexec as "file.bat" and hide it. file.bat contained the autoexec commands we needed to connect to the network. The autoexec file was also hidden and contained the line "File Not Found". When executed, it ran the command "file.bat". Now the prank: our PCs had a built-in speaker and we used Lotus Notes for email. My assistant added a wav file with a fart sound to the office admin's computer for the new mail sound. The computer was on the floor and every time a new mail came in, it farted. This went on for more than two weeks. The really funny part is she was a prim and proper person and asked me to look at her computer. It was making a poofing sound. I went and listened, and told her I didn't hear anything, "it must be your imagination." The whole office knew what was going on. Good thing she had a sense of humor - she was the director of finance's admin. He loved the prank.

**Roger**

*One of the things truly wrong with the present day is that there just aren't enough pranks taking place.*

**Dear 2600:**

I could scarcely have asked for a better example of sanctimony than the editor's counter-argument that the purpose of the word "disinformation" is as a shield against "endless debate" with an "endless batch of people who need to be convinced." But in the context of my original response that sanctimony isn't a curable condition, allow me to offer a piece of advice to falsify my own claim. Debate can end on its own easily enough on the merits of the argument. But if getting the last word tastes

better going down, try these on for size.

"I have spoken." - Kuiil, from *The Mandalorian*

"I will say no more." - Théoden from *The Return of the King*

"Loser says what." - uncredited

**!H**

*We can work with all of that.*

**Dear 2600:**

Looks like hacked@2600.com isn't a valid email address i.e., contact info on [www.2600.com/hacked\\_pages/](http://www.2600.com/hacked_pages/) is misleading.

"Your message wasn't delivered to hacked@2600.com because the address couldn't be found, or is unable to receive mail. The response from the remote server was:

550 5.1.1 : Recipient address rejected: User unknown in local recipient table"

**JC**

*Guilty as charged. We haven't looked at those pages in forever and that alias must have gotten wiped at some point. We've added it back, so it won't bounce anymore.*

**Dear 2600:**

My barely 20-year-old self would always rejoice finding this tiny zine on a Barnes and Noble shelf or in the airport while I was in the Army and stationed in relative isolation in Alaska. I was engulfed in an expectation of strict obedience and purposeful ignorance, and I took my rebellion where I could find it. Fifteen plus years later, I find myself feeling similarly and appreciate that this effort still exists with people still supporting it when I went looking for it. Keep it up.

Happy hacking.

**Jake**

*It's great to know that we were able to help people such as yourself in what must have been a challenging time. We can only hope that we still have that effect in a number of places.*

**Dear 2600:**

Thank you Matt for the intriguing article on Apple's Gatekeeper in issue 41:4. It's a reminder for all of us to stay current with modern operating systems and programming languages. I look forward to more engaging content about iOS, Android, and macOS. After all, we are living in 2025.

**\_claes**

*We can't overemphasize the value of letting us and the author know their article was worth the effort they put into it. Thanks for taking the time to acknowledge this one.*

**Dear 2600:**

First, thank you for publishing my article "A Response to a Call to Arms" (41:2). Second, as I witness the changes in this country that have happened, I feel that we will be entering a time that will have a lack of accessible and truthful knowledge. As I see our own government rip down information, I can't help but wonder how

long we will have a free, uncensored Internet, not 100 percent controlled by big tech. I worry about how long it will be before libraries no longer get the funding to stay open, or are so censored that you can't get any meaningful knowledge from them. Do I need to prepare to figure out how to distribute information to others, loan books that give alternate views, have offline copies of peer-reviewed knowledge that can be used to look up fact-based information? We are entering troubling times. I see the criticism 2600 and *Off The Hook* receive about having to dive into politics, but let's be frank: to ignore it is to not face the problem. Maybe someday we can build a world where we don't have to worry and actively campaign against injustice or fight for access to facts, and we can all sit around and just talk about technology and hacking. But what is needed right now at this point (and you can correct me if I'm wrong - I'm open to criticism of my viewpoint) is for us to take the skills we have and apply them to help those around us, and start fighting for what we believe is right. Expose the corruption of the situation we are in.

**Just Keep Things Anonymous**

*We couldn't have said it better. To not pay attention at this moment in history would be a grave disservice. To not fight to protect and preserve the institutions that matter says that you simply don't care. We are not and have never been immune from having our society completely destroyed as so many have been in the past. And there is a true threat from the global instability that will result from our continued spiral into mayhem.*

*Technology will play a very big role in whatever is ahead. As we have said for decades, the tools that technology brings us can be used for good or for evil. And there isn't a government in the world - past, present, or future - that wouldn't want more power than they needed. So we're well aware of the scenarios we're facing. We all need to help ensure that the knowledge gets out there and that we don't let everything we've built fall apart and disappear.*

**Dear 2600:**

After your last *Off The Hook Overtime* (2/5/25), when you signed off ("mess with the best, die like the rest"), I began to rewatch the 1995 movie *Hackers*. I have watched the movie many times, but this time I noticed something new. It's during the scene in which Dade Murphy (Zero Cool/Crash Override) attempts to take over the OTV television network. Murphy preempts a TV show of a man who looks like a used car salesman wearing a loud and ugly plaid jacket, spouting racist ideology - and when the camera shifts to the videotape of the show being removed mechanically from a



tape player, we see the show is called "America First." Here is an image.



How had I not noticed this before?

As we know, America First was the antisemitic, isolationist, pro-fascist organization affiliated with Charles Lindbergh, founded in 1940 (actually the America First Committee) - and a name resurrected by current fascist-in-chief Donald Trump's former senior adviser Stephen Miller with his America First legal organization.

My favorite response to America First is the immortal line from Woody Guthrie's "Lindbergh."

*"They say 'America First,' but they mean 'America next!'"*

The song ends this way:

*"So I'm gonna tell you people, if Hitler's gonna be beat*

*The common working people have got to take the seat*

*In Washington, Washington*

*And I'm gonna tell you workers, 'fore you cash in your checks*

*They say 'America First,' but they mean 'America Next!'*

*In Washington, Washington"*

Thanks for all you do.

**gmachine24**

*And thanks for all the history you wrapped up and presented as something incredibly relevant to the present. This is exactly what we need more of.*

**DOGE Antics**

**Dear 2600:**

Regarding the recent DOGE activities: phrases like "freaking out" are, not surprisingly, used to describe the reaction of the engineers who were responsible for maintaining the code base until a week ago. The changes that have been made all seem to relate to creating new paths to block payments and possibly leave less visibility into what has been blocked. I want to emphasize that the described changes are not being tested in a dev environment (i.e., a not-live environment), but have already been pushed into production. This is code that appears to be mainly the work of Marko Elez, who was first introduced

to the system probably roughly a week ago and certainly not before the second Trump inauguration. The most recent information I have is that no payments have as yet been blocked and that the incumbent engineering team was able to convince Elez to push the code live to impact only a subset of the universe of payments the system controls. I have also heard no specific information about this access being used to drill down into the private financial or proprietary information of payment recipients, though it appears that the incumbent staff has only limited visibility into what Elez is doing with the access. They have, however, looked extensively into the categories and identity of payees to see how certain payments can be blocked.

Also, how likely is it that Elon Musk is training his AI models on your private financial tax data - like your name, address, income, and more? Or with the Department of Education info like your child's personal information?

**Joseph**

*There is so much that is wrong here. Working in secrecy with unvetted people who have almost no experience in government and no apparent concern for the privacy of those whose data is stored in the many systems they've been given access to. Add to that their ignorance of the data they're looking at, coupled with the massive dollar amounts of alleged savings they were responsible for - only to have those numbers quietly erased when they turned out to be completely wrong, and it becomes apparent that this will go down in history as one of the biggest data breaches of all time. The fact that it was planned by a government against its own people makes it even more special.*

**Dear 2600:**

"This is the largest data breach and the largest IT security breach in our country's history - at least that's publicly known," one contractor who has worked on classified information security systems at numerous government agencies was recently quoted as saying. "You can't un-ring this bell. Once these DOGE guys have access to these data systems, they can ostensibly do with it what they want."

**Rob**

*The damage is incalculable. Having had unfettered access for so long while kicking out the legitimate users is a worst case scenario. Even if the intruders are eventually excised completely from the systems and prosecuted to the fullest extent of whatever law remains, we will never know for sure how many back doors or how much malware exist undetected. Remember, these people were never vetted.*

*To many of the idiots who support these developments, actual legitimate users are now somehow the enemy along with such concepts as science, diversity, and education. We would never trust one of our systems that had been compromised in such a manner. It's foolish for anyone to put any trust in whatever we get back once all this craziness ends.*

**Dear 2600:**

Someone - anyone - regardless of who is in power - why are so many people pro-government all of a sudden. 2600 has always been anti-government across 41 years and eight different presidential administrations. When did the youngins want to incarcerate Kevin instead of Free Kevin? Why would they be against the idea of 2600 winning against the MPAA? The youth of America disappoints me.

**A Fan of 2600 and Off The Hook for 30 Years**

**Brent**

*We, too, are frustrated with the many people who are blindly pro-government lately (although pinning it on the young isn't really fair). Despite data breaches like what's described above and all kinds of other blatantly illegal and unconstitutional actions, they fall into step and regurgitate what is coming down from the top of the government.*

*But there are also many who accuse us of somehow being pro-government when we criticize what is currently going on. It makes as little sense as the actions we're critical of. It's as if they've lost track of who is actually in charge.*

*We stood up to Elon Musk's bullying tactics and helped get the word out through social media regarding who the people were who were secretly taking over government institutions. We intend to be a thorn in the side of this regime for as long as we are able. We've generally done this kind of thing since we started, but we'd be lying if we said the past was at all similar to the present.*

*And, for the record, there were plenty of people in the hacker community who wanted to see Kevin locked up and who didn't support our DMCA case. That's the nature of a community; there is always going to be dissent of one form or another.*

**Dear 2600:**

Court filings say that Mr. Elez was "mistakenly" given write access to the Treasury Department system that is responsible for five trillion dollars of spending per year. And that he and others on the DOGE team came in with the stated goal to "block foreign aid payments... and to automate some of its functions." That sure sounds like write access to me. So, let's assume we're in a capture the flag game. You know you're going to have a

few minutes/hours of read/write access, then it will be removed and changed to only "read" access, and you're supposed to deny that you did anything. How many ways can we think of to get write access again, and/or what damage can be done in those few hours that can then be covered up? I am not reassured.

**Elonka**

*You are quite wise not to be.*

**Dear 2600:**

It's funny that the most recent revision in the procurement forecast for 2025 ([www.state.gov/procurement-forecast](http://www.state.gov/procurement-forecast)) has the largest single line item payee being Tesla for 400 million for a fleet of "armored Teslas." Conflict of interest yet? Straight from the horse's mouth itself, no intermediaries. But DOGE isn't saying anything about this bit of cronyism.

**WKA**

*At press time, we have people in charge who have escaped justice numerous times and who believe that they can do whatever they please and that laws don't apply to them. They've even said this out loud. They're no longer trying to hide their corrupt actions. So a conflict of interest like this is abhorrent, but hardly surprising. That doesn't mean that we shouldn't continue to dig up every bit of evidence that shows what they're up to. They may have set up a very impressive long game that will protect them for now. These things have a way of crumbling into dust when the mood of the people changes.*

**Dear 2600:**

DOGE is definitely making things more efficient - for our adversaries (cyberintel. [substack.com/p/doge-exposes-once-secret-government](http://substack.com/p/doge-exposes-once-secret-government)).

**Shawn**

*This piece sums it up well: "Over the past month, an unprecedented number of critical government systems, including those at the nation's nuclear research labs, have been exposed to the open Internet. This exposure jeopardizes both U.S. national security and the privacy of millions of Americans."*

*We will be dealing with the aftereffects of this intrusion for a very long time.*

### **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](mailto:letters@2600.com) or 2600 Letters, PO Box 99,  
Middle Island, NY 11953 USA

# EFFecting Digital Freedom

by Joe Mullin

## **U.K. vs. Encryption: What Does It Mean For Privacy Worldwide?**

The encryption backdoors are here.

Earlier this year the U.K. government pressured Apple to provide access to end-to-end encrypted cloud backups, or what Apple calls “Advanced Data Protection (ADP).” Instead of complying - which would introduce an encryption backdoor into iCloud backups - Apple has chosen to remove the encrypted backup feature for U.K. customers entirely.

The change makes U.K. customers more vulnerable to surveillance and malicious hacking. But this is just one skirmish in a crypto war that’s been ongoing for decades. Since the 90s, law enforcement and national security agencies in Western democracies have been engaged in a misguided push to undermine encryption. EFF and other advocates for strong encryption have pushed back, pointing out that there’s no backdoor that only works for the “good guys” (and never will be).

Even though this demand was made by the U.K., if agreed to it would amount to a blanket, worldwide backdoor. Any backdoor built for any government puts everyone at greater risk. Just last October, millions of U.S. communications were compromised by the Salt Typhoon hack, in which a Chinese government-backed hacking group was able to infiltrate some of the same “lawful access” systems built by U.S. Internet service providers for law enforcement.

### **How We Got Here**

In 2016 the U.K. passed the Investigatory Powers Act (IPA), also known as the “Snooper’s Charter” because it grants the government broad surveillance powers, including the ability to compel companies to facilitate government access to private user data. According to news reports, this is the authority that the U.K. government tried to use to force Apple to weaken ADP.

Apple’s Advanced Data Protection feature, introduced in 2022, ensures that files stored in iCloud - including backups, messages, and photos - are end-to-end encrypted, meaning that not even Apple can access them. End-to-end encryption is already applied, by default, to photos or chats sent in iMessage. ADP just makes iCloud backups as secure as those chats and photos.

Faced with the choice of weakening encryption for everyone or removing the option of ADP for U.K. users, Apple chose to degrade its offerings in that country. Apple has had a long-standing promise that it will never build a backdoor into its products or services. But by throwing out its

strongest level of encryption in one country, it’s rung an alarm bell to tell us all that our privacy and security are at risk.

### **Ramifications Around the World**

There’s no doubt that other countries - including non-democratic regimes - will look to the U.K. backdoor as an example to be followed. At this point, users in any other country can use ADP; but police in other countries will want the same type of access that U.K. officials have demanded. The French parliament is currently debating a proposal to degrade encryption in the name of fighting drug traffickers.

Weakening encryption not only puts us all at greater risk of identity theft and fraud; it violates fundamental human rights. That’s not hyperbole: last year, the European Court of Human Rights ruled that government-required encryption backdoors that weaken encryption can lead to general and indiscriminate surveillance of the communications of all users, and violate the human right to privacy. Encrypted communications are the digital world’s closest emulation of private, in-person conversation. That’s something we all have a right to.

### **What Users Can Do Now**

Apple is fighting the order. But for now, the removal of ADP means iCloud backups of Apple users in the U.K., are more vulnerable to government access and malicious actors. But Apple isn’t the only company offering end-to-end encrypted backups. Chat backups in WhatsApp as well as backups from Samsung Galaxy phones have end-to-end encryption options that can be enabled, as do many chat apps, including Signal.

For Apple users outside the U.K., now is a good time to turn on ADP if you haven’t already, and encourage others to do so. A few additional steps are required, including either creating a recovery key for your data (since Apple won’t have one) or designating a person as a trusted contact. In addition to providing more protection for yourself and those around you, the spread of end-to-end encryption also creates a new political reality: the more people who use the feature, the harder it will be for governments to shut it down.

We must demand that our governments oppose encryption backdoors. Digital rights organizations like EFF offer advocacy tools that make it easy to contact your elected representatives and speak up on behalf of encryption. We can and must tell our own leaders that we won’t accept the path the U.K. has gone down - a road that makes its own citizens less safe and less free.



# What is The Hacker Ethic - Redux

by Lexi Conn

[lexi.con.thoughts@proton.me](mailto:lexi.con.thoughts@proton.me)

Who are we, what is our ethic, and how does that fit into the times we now live in? Most of all, are hacking and politics/advocacy really separate line items, or are they so co-mingled that we cannot talk about one without addressing the other?

It is the beginning of February when I am writing this, and the events of the last several weeks since the inauguration have prompted me to reexamine what all of this means to each of the communities I am a part of, not just the hacking community in isolation.

I spent my life pursuing science and technology. It's been a passion of mine since I could first walk and speak. My dad was a scientist who chose to become an educator and teacher instead of pursuing commercial employment. Our house, and our basement in particular, was filled with a vast library of books on science, mathematics, philosophy, history and art - a treasure trove of knowledge that opened my mind and my world view.

My dad taught anthropology, biology, physics, and chemistry. In addition, he loved history and archaeology as much as science. Our basement was a mad scientist lair filled with chemicals and machines, with skeletons and models of everything he taught. While most kids would dream of toys for Christmas, I would pore over the Sargent Welch catalog, a 1200-page tome filled with delights of science exploration and education.

This was in the 1960s, well before anyone really knew what a computer was, or how that technology would irrevocably change our lives forever. The first device I disassembled was a tube-based baby monitor - I had to learn and understand how it worked (I did manage to reassemble it). Electronics technology back then consisted of the warm glow of tubes, and the smell of grease and ozone during operation. Tracing circuits without a schematic meant painstakingly following discrete components soldered in place with point-to-point wiring.

And oh, how he encouraged that pastime. Once I learned how to ride a bike and gained mobility, he showed me how to ride the urban allies to search for discarded radios, televisions, anything with electronics. From there I met another kindred spirit, and we would dumpster dive behind engineering firms and device manufacturers. If I found something too heavy to drag back home, he would drive me to the spot in whatever alley I discovered my newfound treasure and would cart it home waiting for me to disassemble.

I learned mechanical engineering this way as well. I once took apart this huge mechanical calculator/computer the size of a large IBM Selectric. It took me two months to learn and understand how all of the levers, gears, and springs could perform the magic of this mathematics calculator/computer. For weeks I could not shake the smell of lubricating oil and grease, but I didn't care. I was in heaven.

What I really took away from that formative experience was so much more than knowledge itself; I eventually learned how to put things back together after disassembly. From there I learned how to repair and even create my own creations. That led to my first foray into hacking; I learned how to modify and improve the objects of my experimentation. It solidified the foundation for what would become a very successful career in engineering.

Nothing comes for free, and this was no exception. There was an equally dark side to my childhood that had as much impact in molding and shaping the person I became. I had known since I was around age five that my biological gender did not match the gender I truly am. Growing up in a house whose parents were both teachers, I innocently believed that I could share all of my true self. Tragically, that proved not to be the case, and therein formed the schism that would separate and isolate me from my family. In that time, I did not possess the vocabulary to express I was transgender; I thought of myself as defective, a freak of nature, something that demanded the villagers to hunt down the likes of me with tiki torches and pitchforks. I was, for all intents and purposes, a gender Frankenstein.

Every parent's dream, at least in theory, is to prepare their child to blossom and prosper as they go out into the world. To have a voice and use that voice to form their own unique identity. To form their own ideas, morals, and values that will prepare to participate in society in a way that benefits everyone, and allows them to express their own "self." Or so you would think....

Except that's not how my childhood played out. As long as I engaged in activities that were deemed socially and culturally acceptable, I was out of harm's way. And so, I had to learn to practice stealth; I had to act one way in public, while desperately searching for like-minded individuals and communities where I would be accepted. Thus laid the seeds for the next stage of my development.

This is the point in the story where the typical "Hacker Perspective" tale begins. By the time I was 11, I was aware of the newly budding

computer hobby. I read a myriad of articles on the Altair, the IMSAI, the RCA COSMAC Elf. I filled my bookshelves with catalogs from PolyPaks, Delta Electronics and John J. Meshna, and with brochures from Ohio Scientific, Processor Technology, and SWTPC. I read a myriad of articles in *Radio Electronics* and *Popular Electronics*. I wanted to be part of this! The flame had been lit.

The first computer I laid my hands on was an Apple ][ through a family friend. I taught myself Integer BASIC, and learned how to program the machine to display graphics in "sprites." By the time I graduated high school in 1981, I had "acquired" a TRS-80 Model III. The seeds started to germinate.

The game changer came in my first year of college. All engineers had to take a Fortran 77 class. That meant having to register for time on the school's IBM 360 mainframe, and waiting for printed output stuffed into shared bins with the other students. There had to be a better way.

I found that way! The school had 300 baud dialup lines, which would allow anyone with VT100 (or similar) or a micro computer running a terminal program to connect. A line printer attached to the computer would provide the printed output.

There was one problem... I could not afford to purchase a terminal software package. There was an assembly listing in one of the many books provided by Radio Shack for the Model III, but I lacked a Z80 assembler. I "acquired" a copy of Radio Shack's EDTASM (editor/assembler), typed in the program, compiled it, and tried to run it. No dice.

It was at that point that in order to find the bug(s), I had to teach myself Z80 assembly language. I obtained the schematics for the RS-232 board, found the specs for the UART chip, figured out the bugs, and voila! I had a running terminal program. Bare bones at best, but it worked. I borrowed an acoustic 300 baud modem from another friend; I was online! No trips down to school to do the assignments.

Around that same time, I came across a list of local BBS's in my area. Intrigued, I started dialing up and logging in. Holy fuck! Where once I was blind, now I could see.

I wanted to learn more! It didn't take long to discover that there were hacker boards and pirate boards (sometimes the same BBS); there were BBS's everywhere just waiting to be explored. It also didn't take long to figure out the gifts of Allnet, Sprint, and MCI to reach beyond my locality. Suddenly the world was my oyster. Ghostship I and II, the TARDIS, Gandolf, Most Significant Byte, it was all out there. I still have a shoebox of 80 track double-sided double-density floppies spilling over with text files, the stuff that

would later become 2600.

It also opened another door I had not anticipated; I found other folks in the queer community, and more specifically, folks like myself. All rejects from society, all blazing our own trail without the permission or approval of the society in which we lived. That experience greatly influenced how I acquired my technical and hacking knowledge. We didn't stop to ask the question "how do I become or learn xxx?" They say necessity is the mother of invention, and there is no greater necessity than survival. It never occurred to me to ask "how do I learn xxx?" in the hacker community... that too was a matter of taking risks to ask and learn, but more importantly, to do the work! Without effort, in any pursuit, you won't get far.

From college into the work world, I was living three lives: The life in public that my family and community saw, the life of who I really am as transgender, and the life in the hacker world. And oh, what a balancing act. Like all juggling acts, there comes a point where you can't keep all of the plates spinning forever.

I tried to put the last two lives to rest, and be "normal." I got married, had a kid, then divorced. I tried to live the life my family and childhood friends expected, but that all began falling apart. At that point, I had a successful career and business, but everything else around me was falling apart.

About ten years ago, everything came to a crisis point. I needed to be who I really am, all of who I am, if I was going to survive. No more living in the shadows; that just wasn't working anymore. I started my transition and began living full time. Legal name change, body changes, the whole nine yards.

I was working for a major large company as a hardware/software engineer, in what had been a very privileged male-dominated "tech bro" world for most of my entire career. It was at one of those shops where I came out as trans. My life has never been the same. Many of my friends and family have excised me from their lives; I am no longer welcome. It was then I decided a fresh start was needed. I moved 2000 miles away to a new city and, quite literally, started over.

To say things have been challenging would be a gross understatement, a disservice to those whose footsteps I was following in and to those who follow in mine. But it also gave me a new resolve to use my skills, *really* use my skills to help others. I was always involved in advocacy of all kinds, but now it had even more purpose.

In addition to the LGBTQ+ community, I pushed advocacy for who we are as hackers, to push back against the stereotypes and the bad actors who wear the title but are far from practitioners of the practice or spirit. To educate

the public on who we really are and what problems we are trying to solve.

A funny thing happens when you take a risk and shed the fear of authenticity. You no longer care about others judging you by their own metrics. You take back your agency and own your own individuality without apology.

Which bring us full circle to where we now find ourselves in this moment in time. As hackers, we have to not just strive for the truth, but insist on shining a light into the darkness of lies, deceit, and conspiracy. Where our mission is to push the limits of technology, it is incumbent upon us to raise our voices against the denial of science and “alternative facts.” Our community has been fighting the good fight against the narrative of corporate greed and control by our three branches of government. At no time has this been more critical than the dystopian reality we currently find ourselves in.

Given the inextricable co-mingling of science and technology with bro-ligarchs making policy for the rest of us, we no longer have the luxury of choosing the former while blindly ignoring the latter. These sycophants of a self-proclaimed orange god are exerting their power, wealth, and influence in every facet of our lives: how we communicate, how we use our dwindling

purchase power, which voices get amplified and which are silenced. We have never been under greater threat than the place we now find ourselves.

So what is the hacker ethic? What does it mean to be a hacker?

At its most basic core, the hacker ethic is about removing the obstacles and artificial limitations that impede the pursuit and practice of advancing our technological and philosophical skill set to remove barriers to entry, and to empower everyone to educate themselves with facts. It allows any of us to unlock our potential to expand our minds, and to solve the world’s most difficult and challenging problems without the societal limitations. It shatters mythical boundaries that divide us, and uplifts anyone who wishes to be a better version of themselves without fear or favor, without regard to race, ethnicity, gender, or sexual orientation. In short, it encourages and rewards us for continually striving to be the best version of ourselves in every moment we draw breath from cradle to grave.

*The Washington Post’s* masthead states “democracy dies in darkness.” So too will the hacker community if we ignore the warning signs, and fail to take notice and take action. After all, isn’t change what we embrace?

## Take Me Out to the Reverse ATM

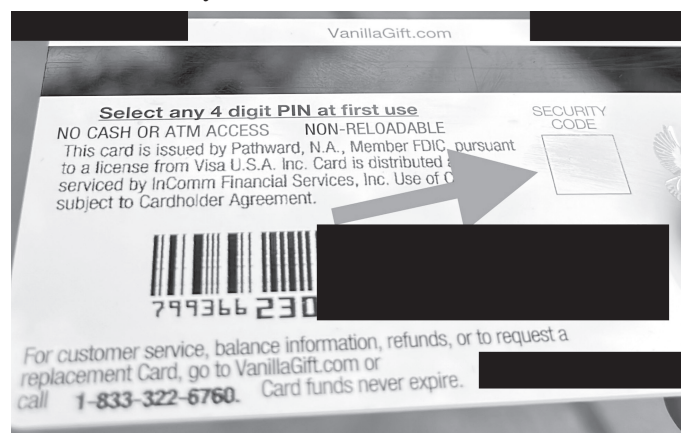
by heyczerny

In the world of OPSEC, anonymous payment methods are an important part of protecting one’s privacy when interacting with merchants. In the physical world, one common tool is the prepaid debit card. This is basically a gift card which can be purchased with cash without providing ID. I have been a fan of Vanilla Visa cards and over the years they have served me well. Recently, however, I have noticed a steep increase in “draining attacks” with these cards, including an alarming trend of cards hitting store shelves with the security code already scratched off and/or mag-stripe already demagnetized.

These attacks are a stark departure from one seen in years past, where criminals steal an unactivated card from a store and create a sticker matching its loading/activation barcode. In this attack they then return to the store and place this sticker over the same barcode of unsold cards still on the shelf. When a victim pays for and activates a card that contains this fraudulent bar code sticker, the money is instead deposited on the original stolen card. Checking for this by inspecting the packaging and looking for stickers is simple enough, but newer attacks involve stealing the card numbers and then

scratching them off, and then demagnetizing it so that the person who actually buys it is unable to use the card.

Sometimes, incredibly, the packaging is still pristine, with no sign of tampering. At one store last year, I explained the situation and asked a manager if he would let me open up the packaging at the register before deciding whether to load it with cash. I brought up a perfectly sealed Vanilla Visa card and we opened it at the register to discover the security code was scratched off. He couldn’t believe it. I walked out without a card. Too risky.





Apparently I am not alone. In the last year, at least two separate lawsuits against various companies involved in the sale of Vanilla Visa cards have been filed. It was time to look for a better solution.

In a seemingly unrelated story, I have watched with much sadness over the years as the ability to anonymously attend a staple of American culture, the Major League Baseball game, has all but disappeared. Not long ago, you could pay cash for a physical ticket at the box office. But as ticket fraud rose and COVID-19 made businesses reevaluate technical solutions, the MLB has locked tickets down hard. Today, to get past the gates and into the ballpark near me, the MLB app is required, and its ticket is both animated and incorporates a rolling code. No more print-at-home. No more screenshots. And once you're inside, it's 100 percent cashless. But if you were to look closely at the amenities, you might notice another new addition to game day: the Reverse ATM.

It works exactly as it sounds. To quote one article, "You insert cash into the machine and it uploads the amount onto a prepaid Mastercard... If you do not use all of the funds during your time at the stadium, the card can be used at your local gas station or anywhere Mastercard is accepted."

This sounded perfect. But I had questions. Was some sort of account required? Would I be asked to scan an ID? To answer these questions and hopefully end up with such a card that suited my purposes, I would need to embark on a mission: Go to an MLB game anonymously and find the reverse ATM.

Creating an MLB account was easier than I expected. I provided a masked email address for this specific task, and password. A birthday was also asked for. I gave the birthday of a famous retired MLB player. Interestingly, a name was not asked for. This signup was done in a privacy-hardened browser over a public VPN. So far so good.

At this point, it was time to find a ticket. Unfortunately, the stadium seat picker would not load in the browser. Maybe it was the VPN, maybe my extensions or settings, who knows? But I would need to move to the MLB app earlier than expected.

I have an old Pixel 3a with GrapheneOS for these sorts of things. It has an anonymous Mint Mobile SIM, and Wi-Fi and Bluetooth are always off. Because it is so old, it no longer receives any updates. I was worried this might cause an issue, but luckily it did not. I installed the MLB Ballpark app and logged in. Browsing for tickets worked fine on the app. I picked a game for the middle of the day in the middle of the week. This way I expected there to be fewer attendees and

thus I could fuzz my actual seating a bit. There's good plausible deniability here - a seat is located by three distinct numbers! Maybe I just got confused.

Paying with a virtual masked credit card and using the stadium as the billing address was accepted, and I had my ticket. It was only viewable in the app, and contained an animation to defeat screenshots as well as a barcode which changes every few seconds. This phone was coming with me to the game.

On game day I put on the team colors to blend in, grabbed my Pixel 3a and hat and sunglasses, and headed out. I noticed a "Will Call" window near the gate which caught my attention since its existence suggested the ability to purchase a ticket app-free. But I was told that while they could maybe assist with a purchase, any ticket would eventually need to be sent to the app. Next it was time to head inside. I was a bit worried that my fake famous MLBer birthday might come back to haunt me as I passed through security, but it was completely uneventful. I was in, the Pixel 3a got turned off, and I grabbed a seat. I decided I would wait until after the first inning to find the Reverse ATM, and during that time I learned a few interesting privacy-related things.

The first is that at a game there is a very slim chance you win one of the random prizes selected for various seats and rows throughout the stadium. I saw free seat upgrades, free food, etc. handed out to various lucky fans as the camera zoomed in on them on the jumbotron. The second is that if you happen to catch a ball at your seat, security might come have a chat with you. This is almost certainly a congratulatory thing, but they might also want some of your information in exchange for that ball. Luckily, I was unlucky in both of these scenarios.

After the first inning, I went and found the Reverse ATM. Interestingly, despite this being a cashless stadium, it was directly next to a regular ATM. The Reverse ATM dispensed Visa debit cards, and loading a new card was as simple as pressing a few buttons on the touch screen, none of which required any data or ID scans. When prompted, you simply insert cash bills up to a limit of \$500. I decided to put \$60 on the card, which I thought should cover a beer and a couple of hot dogs. Unlike Vanilla Visa, there was *no* activation fee. This appears to go against some documentation I found on this card's website, which states potential activation fees up to \$6.00. Perhaps they have a special deal with this ballpark. There is, however, a dormancy fee. The card was printed immediately, and dispensed. I was able to choose a paper receipt as well. I was surprised to see that the card had an expiration date of only nine months from now. I'm not sure if this is by design,

but it is something to keep in mind.



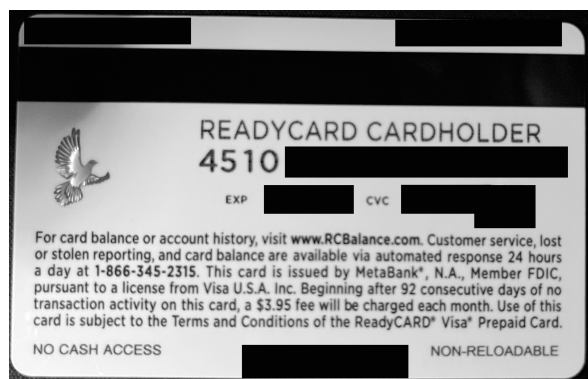
Immediately after the card was dispensed, I took it to go purchase a \$20 beer (I wasn't kidding) and it was accepted without issue. Back in some new seat, I decided to also test it with one of the vendors walking up and down the aisles selling hot dogs. It was accepted there too with no issue after being swiped on his mobile point-of-sale system.

This was mission accomplished. I had come to this game with an anonymous ticket and was now enjoying a beer and a hot dog, courtesy of this new prepaid debit card with no activation fee. I stayed for more of the game, and then headed home. But there were still a few more tests to run.

You may recall that this card is supposed to work both inside and outside the ballpark. So the next day, I made a small purchase at a convenience store and it worked fine. It did, however, ring up as a credit card transaction, which was interesting (but a welcome sign in that it was accepted) and which cost me 38 cents. I think this charge came from the convenience store end and not Visa but I'm not sure.

The final test was an online purchase. Again,

using a hardened browser and a public VPN, I am happy to report that the remaining funds on the card were able to be charged successfully in a donation to the EFF.



Some final notes: Like Vanilla Visa, there is a free website which lets you check the balance of the card at any time. Unlike Vanilla Visa, this website is much friendlier to VPNs. Be aware of short expiration timeframes and any dormancy fees. Also, your experience on activation fees may vary if this was a special agreement between the ballpark and the Reverse ATM company. Finally, be aware that the Reverse ATM *does* have a front facing camera similar to that on an Amazon Locker kiosk. However, it is high enough that a hat brim could likely shield your face.

Hopefully these Reverse ATMs show up in more locations over time. I would certainly use them again. They appear to be a nice alternative to other prepaid debit cards and potentially cheaper as well. Finally, like other privacy tools that grant some level of anonymity, use them responsibly or we all run the risk of them either disappearing or being made ineffective through future identity verification requirements.

## 2600 T-SHIRTS

Do you want to wear this issue's cover? Or any cover from 2020 to the present? Visit [store.2600.com](https://store.2600.com) to see the vast array of hacker-related clothing you can get! (Most are under \$20!)

Feel free to browse amongst our other awesome hacker paraphernalia during your visit.

# INTERRUPTION

by Alexander Urbelis

Reverse Engineering the Trade Wars

[alex@urbel.is](mailto:alex@urbel.is)

With a light that is softer and which has more of a golden hue than the rest of the floors of the establishment, the Strand's rare book room is a special place. Special in its own right, the Strand is the oldest bookstore in New York City (aged 97) and one of the most recognizable names in the book trade worldwide. The hardwood floorboards seem to creak and give just the right amount of bounce to your step, adding a hint of old-worldly gravitas to the ambience. It was there that I sat with my friend and colleague, Nick Johnson, the founder of the Ethereum Name Service, and next to him, another dear friend, Aaron Amendolia, Deputy CIO of the NFL (who you may remember from this column in 40:2), and in front of us, sitting on a leather chair perched on a podium was Cory Doctorow, being interviewed by the comedian John Hodgman. Genius, it has been said, lies not in simply knowing one subject or art very well, but in the ability to synthesize ideas and concepts. It was not shocking that in this heady setting - amidst domestic and global political turmoil - ideas were flowing. It is here that the subject of the strategic and retaliatory repeal of strong-armed intellectual property protections was first broached.

The synthesis of these concepts was not my own. It was a question from Nick to Cory about his prediction as to which technologies would likely be used in unintended ways that the creators of the technologies did not envision and would like to prevent, a common theme throughout Cory's works. The twists and turns of Cory's answer is what brought forth the germ of this idea, which I shall unpack.

Many readers will recall - and many younger readers will likely not recall - the fight that *2600 Magazine* had on its hands in 2000 with the Motion Picture Association of America (MPAA) over the publication of DeCSS, a program written by a teenager that effectively bypassed the monumentally stupid and simple content scrambling system that encrypted DVDs.

Rather controversially at the time, Section 1201 of the Digital Millennium Copyright Act (DMCA) made it illegal to circumvent technological means - no matter how simplistic or idiotic such means were - that controlled access to copyrighted materials. Unscrambling

the scrambled, decrypting the encrypted, or removing whatever measure a copyright owner put into place to protect work would fall under the prohibitions of Section 1201.

The legal saga between 2600 and the MPAA - which ended with the dean of Stanford Law School arguing pro bono on behalf of 2600 in the U.S. Second Circuit Court of Appeals - involved none other than those very anti-circumvention provisions of the DMCA. And sadly, despite the legal firepower at work, it was not a great outcome. The MPAA prevailed in obtaining a permanent injunction against 2600, preventing the publication of the DeCSS source in the magazine. But no one, not even the MPAA, was silly enough to think that a single U.S. law and an injunction against one magazine could stem the free flow of information or prevent a budding generation of reverse engineers from deconstructing their flimsy copyright protection regimes. The MPAA needed help. They needed teeth. They needed leverage. And, over the years, they found all of those things with U.S. Trade Representatives.

This curious office, you may be wondering, is responsible for developing, coordinating, and implementing U.S. trade policies. And the U.S. Trade Representative (USTR) herself acts as the President's principal trade advisor, negotiator, and mouthpiece on all issues of trade involving the United States.

Indeed, with that background in mind, it should not come as a massive surprise that the MPAA lobbied the USTR to negotiate for more active measures for copyright protection of movies. In the name of safeguarding the global competitive nature of the U.S. movie industry, the MPAA pushed the USTR to require stricter copyright regimes as a condition of doing business with the United States. And as it turns out, pressuring foreign countries into adopting strict intellectual property protection laws that align with U.S. values is one of the stronger suits of the USTR.

Since 1989, the USTR has issued something called the Special 301 Report, through which the USTR specifically calls out countries that it considers to be lacking effective protections for American intellectual property rights. Countries on the USTR's naughty list might



face trade sanctions, lose trade preferences, find themselves facing a World Trade Organization dispute settlement proceeding, or have to deal with additional U.S. diplomatic pressure. The very fact, however, that a country may be on the USTR's naughty list can cause reputational damage leading to the loss of trading partners and foreign investment.

Seen in this light, the Special 301 Report (aka the naughty list) is a big stick that the United States can wield against nations that dare to hold differing values when it comes to IP rights. The values with which the USTR happen to wish other nations align are coincidentally those very same principles and measures found in the DMCA that prohibit bypassing technical measures put in place to protect copyrights. Thus, many nations now have some form of DMCA-equivalent legislation on their books.

But this fear of the USTR's naughty list may be subsiding - and national interests may be stronger - than the fear of not being best business buddies with the United States. As the world has watched Trump single out our allies and largest trading partners (i.e., Canada and Mexico) for massive 25 percent tariffs on imports - ostensibly tied to issues completely unrelated to legitimate trade, e.g., drug trafficking and illegal immigration - other nations will inevitably begin thinking that it may not be in their best interest to hitch their economic wagons to the United States.

When other nations diversify their trade partnerships away from being U.S.-centric, this simultaneously weakens the strategic position of the United States and strengthens the relative positions of our competitors, such as China. And in so doing, the USTR naughty list becomes less and less relevant.

What becomes more and more relevant on account of these ridiculous trade wars is self-reliance. When you cannot count on your trading partners to furnish you with the technologies a nation needs to sustain its economy, that's highly problematic and a sufficient reason to reform policies to foster domestic innovation. What may very well fall away are the anti-circumvention and reverse engineering restrictions that nations the world over have put into place simply to appease the USTR and stay off the naughty list.

And there are strategic reasons for a nation to foster reverse engineering: if there is a fear that an inability to source certain materials could disrupt critical supply chains, or if certain essential technologies may be difficult to source, then reverse engineering the functionality of these products begins to look more like an

economic imperative and less like a liability. Thus the embodiment of the phrase, attributed to Hubert Humphrey that "foreign policy is domestic policy with its hat on."

Reverse engineering thus becomes a viable alternative to tit-for-tat tariffs. In fact, tariffs do not even come into play if a nation is able to successfully reverse engineer products and manufacture them domestically, or with the aid of trade partners who do not penalize their allies. If the strictures of the DMCA-like legislation around the world begin to fall, then countries that promote rather than prohibit reverse engineering will gain an economic advantage while the United States remains at a disadvantage.

Reverse engineering will bolster domestic economic growth: it will create jobs, it will increase the share of knowledge that can be spread amongst a local ecosystem of builders and doers, and in so doing, close the technological gap between rich nations and poor nations. What is more, reverse engineering can make otherwise costly products or technologies more accessible and can cause markets to be more efficient - it reduces reliance on monopolies and closed source systems. Ultimately, should it ever come to bear, a global community of reverse engineers who can operate without fear of legal repercussions would break the chain of major U.S. tech company hegemony, all the way from consumer applications to the dominance of the U.S. military industrial complex.

And why should this not be the case? Have we forgotten that ideas are public goods? Does every idea with economic value need to belong to someone or some entity?

Deep within the Strand, possibly in the rare book room, I would bet that one could find the correspondence of Thomas Jefferson, and in that compilation of letters one might come across Thomas Jefferson's missive of 13 August 1813 to Isaac McPherson in which he wrote that, "If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea." Going on, Jefferson argued that "He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper [candle, *archaic*] at mine, receives light without darkening me." This 18th century wisdom - that ideas, like fire, spread without diminishing their source - may not only be the key to defeating Trump's trade wars but could unfetter generations of hackers and builders, unlocking the next level of collaboration and human potential.

# The Cult of Youth

by Bioszombie

In Volume Forty-One, Number Three, “The Burnout Machine” stripped away the tech industry’s glossy facade, exposing its brutal reality. Developers, sysadmins, hackers; it chews them up and spits them out exhausted, disillusioned, and disposable. Burnout isn’t just a byproduct of this system; it’s the design.

And while “The Burnout Machine” laid bare the industry’s relentless demands, there’s another myth that fuels this grind. It’s the Cult of Youth, a poisonous ideology whispering in our ears that if you haven’t “made it” by 25, you’re already behind. The Cult of Youth doesn’t just feed the burnout machine; it’s the myth that keeps it running.

The Cult of Youth tells you that your worth peaks when you’re young. It glorifies the 20-year-old tech founder, the college dropout who built an empire, the “disruptor” who’s barely out of their teens. These stories are more than just distractions; they’re weapons. They set a timeline for your life. It isn’t yours. It never was. It’s a script to keep you running, chasing, grinding - for them.

This isn’t ambition. It’s control.

The tech industry weaponizes the Cult of Youth to keep the machine running. It pushes you to sacrifice your health, your relationships, and your future for someone else’s deadlines. It traps you in a poisonous loop.

If you’re not pulling all-nighters, you’re not “passionate.” If you’re not answering emails at midnight, you’re “not committed.” If you’re not burning out, you’re “not trying hard enough.”

The machine thrives on this mindset. It thrives on making you believe that the clock is ticking, that you’re already running out of time. And when you inevitably burn out, the Cult of Youth whispers, you weren’t good enough anyway.

Here’s the truth: the Cult of Youth is a lie. Your 20s aren’t the pinnacle of your life. They’re the foundation.

The myth that success is tied to youth doesn’t just isolate you; it erases the achievements of those who take the long road. It tells you to admire the spark, but ignore the fire. Linus Torvalds started Linux at 21, but his real success came years later, as his steady, deliberate work built the backbone of modern computing. Margaret Hamilton wasn’t in her 20s when her software put humans on the moon. She was in her 30s, and her achievements weren’t the result of a sprint; they were built over years of careful, methodical effort.

The Cult of Youth wants you to believe that failure is fatal. It isn’t. Every failure is a trace. Every misstep is a log entry. Every crash is a clue.

The Burnout Machine pushes you to sacrifice everything in pursuit of short-term gains. The Cult of Youth tells you that if you fail to meet those expectations, you’ve lost. Together, they create a system designed to keep you grinding and powerless.

The truth is simpler. Success isn’t tied to youth or speed. It’s tied to persistence. It’s tied to the willingness to learn, adapt, and grow over time. The industry thrives on making you feel like you’re running out of time. Hackers know better. The only timeline that matters is the one you set for yourself.

We are hackers on Planet Earth. We’ve spent our lives taking apart broken systems, studying how they work, and rewriting them to our benefit. The Cult of Youth is no different.

Hack it. Exploit its flaws. Share what you learn so others can escape its trap.

The Cult of Youth thrives on isolation and fear. The antidote is connection and knowledge. Teach others what you’ve learned. Show them that the industry’s timeline is a lie. Build tools to help those coming behind you navigate this machine without getting consumed by it.

The Cult of Youth and the Burnout Machine are designed to make you feel alone, like your struggles are yours alone to carry. But they aren’t. We’ve all felt the midnight Slack pings, the “grind harder” culture, the crushing weight of impossible expectations.

We’ve also learned to reject them.

Age isn’t a weakness; it’s a toolkit. Wisdom isn’t a liability; it’s a weapon. With time comes the patience to pause, the clarity to focus, and the perspective to see the bigger picture.

The Cult of Youth sells the spark. Hackers build the fire.

The Burnout Machine and the Cult of Youth are broken systems, and broken systems are meant to be hacked.

Your failures don’t define you. The clock isn’t ticking. You are not running out of time. You’re just getting started.

Mistakes aren’t errors; they’re the blueprint for what’s next. Crashes aren’t failures; they’re the start of something stronger. Hack the timeline. Hack the system. Hack the planet - and build the fire that outlasts them all.

# A Timeline of Recent Search Engine Events (Or as My Father Would Put it, Where Did My Google Go?)

by Kenova Ceredo

kenova.ceredo@protonmail.com

What follows is a timeline of events that is factual to the best of my knowledge. The timeline itself contains no opinions, although there may be some in the conclusion. Most of the events happened in late 2015 and 2016, but there are also some details about the end of the Gigablast search engine, which happened a couple of years later. A few of these events are very obscure, even though they may have had a large impact. I hope you enjoy reading it, and perhaps learn something new. By the way, if you find any of this interesting, you are allowed to take a picture, scan, or screenshot of this article and share it willy-nilly around the Internet, or as a facsimile transmission on the HF bands. *2600 Magazine* is okay with that too, because they printed this permission notice. If, however, you don't find it interesting, you aren't even allowed to read it aloud to other people, and you are encouraged to forget about it completely.

## 2015 - 2016

*July 1, 2015:* The company behind the Gigablast search engine announces that they have entered a partnership with the Internet Archive, and are going to use their technology to index the Internet Archive's vast collection of archived web pages. At the time, the Internet Archive had about 485 billion pages in its collection, and the plan was to index it in order to make "the biggest search engine ever created." ([web.archive.org/web/20151113002432/http://www.gigablast.com:80/blog.html](http://web.archive.org/web/20151113002432/http://www.gigablast.com:80/blog.html))

*Sometime between November 13th and 26th, 2015:* Gigablast removes their announcement about the Internet Archive from their blog page. As far as I can tell, the Internet Archive never made an announcement about the agreement. There is no more news about this, and apparently "the biggest search engine ever created" is canceled. ([web.archive.org/web/20151126032955/http://gigablast.com:80/blog.html](http://web.archive.org/web/20151126032955/http://gigablast.com:80/blog.html))

*February 2016:* Google decides to phase out the "Google Search Appliance" product, which was essentially server hardware running Google's software that allowed the owner to index and search through large document collections. The largest model could store and

index up to 100 million documents.

*Sometime in early 2016:* Google starts limiting all searches to about 400 results, which is about 40 pages. Before this, the limit was about 700 results, and a while before that it was about 1000 results. This is according to anecdotal evidence from a "Diamond Product Expert" on [support.google.com](http://support.google.com/websearch/thread/25885806/header-indicates-thousands-of-results-but-only-110-are-shown). ([support.google.com/websearch/thread/25885806/header-indicates-thousands-of-results-but-only-110-are-shown](http://support.google.com/websearch/thread/25885806/header-indicates-thousands-of-results-but-only-110-are-shown))

As of early 2025, all search engines that I know of limit the number of results that you can see. Some engines like Bing and Mojeek deliver about 1000 results before stopping the user from seeing more, but most of them deliver a lot less. Brave Search, for example, only delivers about nine or ten pages, which translates to about 170 results. Mwmb1.org (a small project with only about 600 million pages in its index) only returns about 80 results. To be clear, these are limits that stay in effect for very broad searches, like "cheese" and "pancake". Unfortunately, I don't have any dates for when the limitations on search engines other than Google started.

*February 6, 2016:* All Seeks nodes become unusable. Seeks was an open source meta-search engine that re-ranked results based on user activity.

*April 2016:* Microsoft starts to open source BitFunnel, which seems to at least be a large part of, but might actually be the entirety of, their indexing system for the Bing search engine.

*April 2016:* Sylvain Zimmer starts the Common Search project that was to mainly use Common Crawl data in its index. Some ranking data from this project was used by Common Crawl (mentioned in this post: [commoncrawl.org/blog/august-2016-crawl-archive-now-available](http://commoncrawl.org/blog/august-2016-crawl-archive-now-available)), and Greg Lindahl (who is now CTO of Common Crawl, but didn't appear to be at the time) was listed as an advisor. There are a couple of small search engine projects still running today that use Common Crawl data: alexandria.org and chatnoir.eu, but the latter only uses two crawls from Common Crawl, and the former appears to draw from



a similarly small index. Two crawls is a tiny fraction of what Common Crawl has available. I do not know if the plan was for Common Search to use the entirety of the available Common Crawl data, but if they had, and if they were still running today, they would have about 250 billion indexed pages, which would put them in the same league as Google and Bing. Some of the pages from commonsearch.org are available on the Internet Archive, but a more complete and current archive of the site is available on Github: [github.com/commonsearch/cosr-about/tree/master/content](https://github.com/commonsearch/cosr-about/tree/master/content).

*August 2016:* The last blog post for Common Search is posted. No more work is done on the search engine past this point. There is currently no mention of it on the founder's website ([sylvainzimmer.com/](http://sylvainzimmer.com/)).

*October 2016:* Microsoft appears to abandon work on open sourcing BitFunnel. No more blog posts are made about their progress past this point, even though no official statement has been made about canceling the project. A paper about BitFunnel is published in August 2017, but it does not appear that any work is resumed on the project. ([bitfunnel.org/](http://bitfunnel.org/))

### **End of Gigablast, 2018 - 2023**

*January 2018:* [gigablast.com/faq.html](http://gigablast.com/faq.html) is replaced with a blank page. Before it was blank, the page detailed some features and technical specifications of the search engine, and explained how to install the Gigablast software on your own computer and get it up and running, in order to have a local instance of the search engine with a personally constructed index. If you visit an archived version of the page on the Internet Archive, you can actually still download and install the linked Gigablast binaries, because they were archived as well. I have tested the Debian/Ubuntu 64-bit version, and it seems to work well except that it doesn't support SSL, so any pages that require HTTPS will not be crawled. I have been told however that the original version of Gigablast ran behind an Apache2 reverse proxy, which took care of SSL. I have not attempted to set up such a system myself, but it may be a fun project for the interested reader.

*Sometime between February 26 and March 9, 2022:* A small message is placed at the top of the Gigablast home page and blog page, which consists of the words "Fuck all dictators!" beneath the United States flag. Sometime between March 19 and March 23, the words change to "No more dictators!" Sometime between April 6 and April 28, the flag goes away and the words are replaced with "sudo rm -rf /dictators". Sometime between September 11 and October 30, 2022, the message disappears and doesn't come back. I am not sure why these messages were put here, but perhaps they can fuel my readers' speculations as to why Gigablast eventually went offline.

*Early April 2023:* [gigablast.com](http://gigablast.com) goes offline completely and permanently with no announcement.

I don't know why most of these things happened. I don't know why many happened around 2016, or if that is just a coincidence. I don't know if any of these people ran into technical issues, or legal issues, or what. All of the outcomes of these events concern me however, and I would like to know more about all of them.

If you have any comments, facts, theories, hints, tidbits, stories, insights, or anything that seems remotely related to this subject and might be slightly interesting, I want to know about it. Heck, even if it seems unrelated and boring, but this article reminded you of it, let me know. Please contact me at the email address specified under the title of this article, or let the whole 2600 community know about it by sending a letter to the editor. Or do both. You can use an anonymous remailer (if you trust any of them) if you are concerned about identity.

Anyway, I hope I added to your knowledge, and I hope you're healthy and having a great time. I feel an urge to toss around vague statements, so I'll say this: Sooner or later, somebody needs to do something that makes stuff happen. Maybe a lot of people need to do stuff before something actually succeeds. Maybe one of those people could be you. If you try anything, I'd like to hear about it.

## **WRITERS NEEDED!**

Send your articles on hacking & technology  
to [articles@2600.com](mailto:articles@2600.com)

# Cybersecurity Can Be Expensive

by lg0p89

Cybersecurity tends to be expensive. Staffing (i.e., quality, experienced staff) is not cheap, especially with the shortage from the numbers needed. The delta between supply and demand continues to grow. The tooling continues to grow in complexity and cost. Depending on the use case, the business may even need more than one tool to cover all the required areas, even if there is a slight redundancy.

When there's an issue, aka compromise, there tends to be an uptick in costs. These can come from various sources, including new cybersecurity tooling, hardware, third-party forensic teams, and everything else.

For the third strike, there can be costs much later. The compromise could be caused by the infamous click-happy user, or better yet the user who receives a call from someone in IT asking to remote login into their system. In other cases, pentests had been done with some vulnerabilities being found over and over. With the latter case - and when there is a serious lack of security controls - there can be fines.

This was also the case with Lewis & Clark College in Portland, Oregon. This is a private liberal arts college and has three primary schools (College of Arts & Sciences, Graduate School of Education and Counseling, and the School of Law). There are approximately 2100 undergraduate and 1400 graduate students. The costs for the compromise were direct and indirect. The direct costs are the immediate costs after the compromise that can be directly attributed to the issue. These are all the people working extra/overtime, the extra tooling for present vendors, new tools that should have been purchased three years ago, and contracted parties to assist with the remediation and forensic work. What's generally overlooked are the indirect costs. Lewis & Clark College is finding this out the hard way with a class action lawsuit based on the compromise.

## Background

A compromise of this nature, depth, and magnitude doesn't happen every week. On or about February 28, 2023 the college experienced a cybersecurity incident. The adversary was able to compromise the perimeter and network security and accessed the crown jewels, here the college's data. Once the issue was detected, the college started sending urgent messages on social media and posting other messages on their website stating their systems were down, which started March 3rd. The systems affected included Workday, Google Workspace, Box, Moodle, GoAnywhere, Classroom Technologies and others. This lasted until March 7th.

## Post Incident

The IT operations certainly became busy when the hints of the compromise surfaced. Once the full

scope of the compromise began to show, the college worked towards securing the network, along with other actions to mitigate the attack's effects. The college also engaged third-party cybersecurity professionals for their forensic work.

Once the forensic team had access to the systems and logs, they were able to confirm the data which had been exfiltrated by the adversaries. While they did have the data, there was no evidence yet that the data had been maliciously leveraged. That doesn't mean it won't happen. They were able to determine if the accessed files did have personally identifiable information (PII) or personal health information (PHI).

Due to this, the college did complete the notification on March 22nd with notification letters to each person potentially affected by the breach. In particular, the data included the affected person's name, date of birth, SSN, driver's license number, state identification number (if applicable), passport information, financial account information, medical information, health insurance information, and college unique identifier. This is quite the list of items. I'd describe this as a plethora of data points useful in so many ways. Identity theft would be easy with this in hand.

## The Other Shoe

The successful attack was serious enough and widespread enough that it affected not only the data but also finance, operations, classroom activities, and most other aspects of the college. Approximately a year later, the other shoe dropped and the college received more bad news.

Console & Associates began the investigation into filing a class action lawsuit against Lewis & Clark College due to the compromise and its effects. They are "eager to speak to victims..." Anyone who receives the Notice of Data Breach can be part of the lawsuit.

A former employee of Lewis & Clark College was the plaintiff for the class action suit against the college. A basis for the suit is that the school did not take adequate safety measures and precautions to protect the students' and employees' data. The class action lawsuit alleges the college acted negligently in protecting the data. The suit also alleges a breach of implied contract and a violation of Oregon's Unlawful Trade Practices Act. While this is filed, the court still must certify it as a class action.

This is probably not going to be cheap. The college is going to pay attorneys and paralegals throughout the legal process. There will also be the amount the court will assess the college if found they acted negligently. This isn't going to be a short and quick case. The investigation alone will take a massive amount of time, which translates into a large legal expense. Oh, and by the way, there will be hours of witness preparation to pay for.

# I Took the Red Pill: A Journey to Linux

by tknrn

It's official: I've gone rogue. I've taken the red pill.

For most of my life, I've used Microsoft-related products. From the early days of MS-DOS 5.0 up until this year, my primary platform has always been some variant of Windows. I'm not here to argue whether Microsoft is good or bad, but due to its popularity, ease of use, robust support and ecosystem - Microsoft Windows remains the most widely deployed operating system in the world (as of November 2024), with a 58 point margin over the second most deployed OS, Mac OS X.

This is likely true for many people, considering market share alone. That being said, even at an early age, I was drawn to the open source world. The idealism behind it I identified with, which started as a small flame that eventually grew into a fire. In my early years, I experimented with Mandrake and Red Hat Enterprise in the early 2000s - when package manifests were printed on paper as thin as the Bible. In many ways, that manifest was like a Bible - it was the key to knowing which software could run on the platform.

For years, though, the challenge was always the same: not having access to the software that the rest of the world was using for daily productivity. As an IT professional, I needed to work with Windows-only applications, so it was hard to fully embrace Linux. However, things started to shift when Mac OS X adoption grew, and Apple's iPhone choices began to influence consumer desktop choices. We saw the rise of diversity in the desktop world. Code changes that were made to a new BSD variant helped bridge the gap for companies, making it easier to recompile for Linux. Over time, mainstream software began supporting not just Windows and OS X, but also Linux. We saw apps like Teams for Linux, Zoom, Spotify, Discord, FileZilla, Visual Studio Code, and even VPN clients like Atmos making it easier to run essential tools across different operating systems.

Which brings me to the present day. I reached a point where I was just *sick and tired* of being sick and tired. After decades of reinstalling Windows, struggling with the infamous registry, and dealing with new problems, I simply didn't want to deal with another Windows deployment. The breaking point came when my perfectly modern setup had a laggy keyboard (a known issue) and, after a fresh boot, my memory footprint was already at 75 percent utilization, even with no foreground applications open! It's a laptop - I can't easily solder new memory chips into my HP Envy, as much as I'd love to. But even so, there's no excuse for having a laggy keyboard on a modern computer after decades of development experience.

I took a step back and checked the applications I was regularly using. To my surprise, many of them were already open source applications compiled for Windows. So, I took the plunge. Since it was a corporate laptop, I swapped out the NVMe drive, installed a new one, and set up a LUKS-encrypted Ubuntu system. I've been running Ubuntu for the past few years on my workbench micro computer with good results. In my opinion, Ubuntu has the most robust software repository for an end user desktop setup, so it seemed like the best choice.

The experience has been fantastic. I don't foresee myself ever going back to Windows as my primary workstation. My system's resource utilization dropped to 40 percent with an idle desktop, even with all my applications and autostart features running. Sure, I miss a few applications, like the Adobe Suite and some niche Windows-only software. But for the most part, I've been able to run those with Wine, experiencing no or only minor issues.

There's no better time than now, with the rise of AI, cloud providers, and companies like VMware/Broadcom fueling the interest in open platforms. If my journey resonates with yours, I urge you to take the leap.



# Lee Williams, Harassment Agent

## Episode 5

by Lee Williams

*(This story is a complete work of fiction.)*

Life is short. Make the most out of it.

See me, I don't feel like I'm doing that. I often think about what options I had. I could have played classical guitar in New York. I could have joined Doctors Without Borders. I could have tried going to college. Hell, I could have played shortstop for the Mets. I could have tried a thousand things, yet here I am, a depressed criminal. And lying in a crack den, with the sun shining just barely through the window, I wonder how I got here.

The answer, I guess, is I fell in love with The Fast Life.

Could you blame me? Never a dull moment with me, I guess.

At least, that's how I felt before I was shot at leaving my motel. I walked outside and started walking down the street, when I saw a black Nissan in the parking lot turn on and start trailing behind me. I walked faster and it sped up. I walked even faster and it sped up even more. As it came alongside me, the window opened, and I heard the sound of "Stormy Weather" by Etta James out the window.

Then I saw metal, and heard a shot go off, barely missing me. I dove behind a car, curled myself up behind the engine block as I saw bullets whizz right through both doors of the car. Movies never focus on this detail, but car doors are not bulletproof. The only part of the car that will stop bullets, or most bullets anyway, is the engine block.

I closed my eyes. I'm somewhere else. I'm in Puerto Rico. I'm in Canada. I'm getting drinks with JB. I'm literally anywhere but getting shot at in Jacksonville.

Eventually I heard wheels spinning as whoever that was pulled off. After a few minutes, I cautiously got up. But I heard sirens coming and ran into the bushes. I may have been the victim, but I can't stick around anyway.

Pierre told me where he was, but I had no real way to get there, so I called a cab to the address he sent me. When I got there, it was an abandoned house that made the den I was staying in look like The White House. Although, I mean... with the current climate of U.S. politics....

Bump keys are keys specifically designed for lockpicking. You insert them into the lock, and then lightly bump it with a hammer. This makes the pins jump, and after enough bumping, they

all jump into the right position to open the door. With a full set of bump keys, it's estimated that you can open nearly 90% of all cylinder locks.

And the locks on an abandoned house are certainly nothing special. I opened the door, and was hit with a smell that was a mix of beer, cigarettes, chili, dust, asbestos, and piss.

"Pierre!" I shouted. I was met with silence. "Are you in here?"

Nothing. I walked through the whole house. Eventually I made it to the kitchen, where I saw a note.

Lee

I went to california. Sorry to ditch you like this. Gotta find my lady

Good luck man.

There's a beer in the fridge. Pack of smokes in the pantry.

Thanks for the help.

His Signal is now deleted.

I sat down on the couch and turned the TV on. I guess the power still works here.

"Pavel Durov, creator of Telegram, was arrested in France today, on charges of-"

Change channels.

"The Fentanyl epidemic in the United States continues to escalate, with the death toll in the thousands. Narcan, a drug-"

I turned the thing off and sat. I was overcome by a deep burning anger, a resentment I've never felt before for my situation, an anger directed at everything and everyone that got me here. Ray. Valentina. Pierre. I was so angry that I couldn't even think straight. What do I even do now? I'm in Jacksonville, Florida, running from an organized crime group I gave my life to, poured my soul into, made my entire being, all to be terminated in my very early 20s. My back hurts. My head hurts. My stomach was turning. And now, my last companion aside from JB has gone to California to chase some girl, and I'm just sitting here with absolutely no idea what to do next. What do I even do?

I turned the TV back on.

"Two arrested for going on a shooting rampage in Jacksonville spanning four days, resulting in three deaths. One suspect committed suicide, while the other was taken into custody without

incident. 19-year-old Isaiah Briggs, when questioned by police, said he did it because he didn't like Mondays."

Huh. Now that is one hell of a coincidence.

I decided it was imperative to disappear. And the first step in disappearing is, and always will be, physically. So I booked a Greyhound to Miami to gather my thoughts and make a plan. The only problem was this burning desire to get back at Ray and Valentina and all of them. But getting revenge is like taking poison and expecting the other person to die. Maybe that's why I made it my trade, to avoid my own desires to get back at the ones who wronged me. Because when I'm doing it for someone else, it's nothing personal.

Really, it isn't.

I bought the ticket with something called a "bank drop" which is basically a bank account fraudulently set up under someone else's name. It cost me 180 dollars on ToR. I had a matching driver's license. And whoever this is, I also had his SSN. Which is basically everything I need.

Nice to meet you. I'm Anthony Magello.

I called a cab to the bus stop, waited for the bus, and got on, leaving Jacksonville in the dust.

### ***Miami, Florida***

"Hennessy," I said shyly. "And a Modelo."

The bartender, without saying anything, poured a *very* conservative shot of Hennessy and gave me a Modelo, one of the small cans.

"27 dollars," he said.

I paid and angrily sipped my drink. Then, I heard a very confident, booming voice say, "What do you do for work?"

I looked to my left and saw a couple, in their 30s, sitting at the bar. The man was tan, and had a floral shirt on. The woman was short and fair skinned, and had glasses.

"Tech sales," I said. "How about you?"

"Well," he said. "I was the manager of a bank in Arizona, but we got robbed, or not really robbed but stolen from, and I was assaulted in the process. So I sued the bank, won, and I used the money to invest in the stock market."

"Huh," I said. "What do you mean not really robbed?"

"The guy was defrauding us. He had used various tricks to create a fake business account with our bank."

"And he assaulted you?"

"I was trying to distract him," he said. "While the police were coming. And he threw a stack of papers in my face. They never found him. He's presumed dead."

"Jesus," I said. "How much did you get?"

"500k. Then I turned it into a million. Now I count a million every time I blink."

"Every time you blink!?"

"Well," he said. "Not that much. But a lot."

The woman interjected. "You don't work in tech sales."

I was caught off guard by this. Did she know me? Was she with HHH? How did she know I was lying? Is she the cops? The possibilities ran through my mind so fast I forgot to speak.

"Hah!" she said. "I guessed right! Look at your face."

Fuck.

"What's your guys' name?" I asked them.

"I'm Khir," said the man. "And this is Amber. How about you?"

"Anthony."

"So what do you really do, Anthony?"

I thought about it. I thought about this whole rotten adventure, I thought about this entire journey, how terrible it was, how I wished I was dead, how I wished I was caught, how I wished a million things other than this, and said a hail mary. I looked at them. They had this look in their eyes, both of them. You know how the eyes are the window to the soul, well, they had this look that wasn't quite right. And I decided, fuck it.

I sighed, and said, "I was involved in an organized crime syndicate and now they are trying to kill me. And now I'm running from them."

"We'll kill them," said the woman.

I looked at her in shock.

"I'm joking!" she said. "Your fucking face."

I laughed nervously and took a sip from my beer.

"Unless..." she said.

"No," I said. "I'm alright, I think."

"Here," Khir said. "We know a beach bar nearby. And Amber's friend is coming, and I think she'd like you. And you seem fucking lonely. Why don't you come with us, huh?"

I paused. It could be a setup. It could be a trap. It could be a million things. But at this point what did it matter.

"Why not?" I said.

"Awesome," Khir said, with a smile.

"Hey man," I said. "You know you have a good radio voice right?"

"What do you mean," he asked.

"Like, deep. And booming."

### **Soundtrack**

*Stormy Weather* - Etta James

*The Root Of All Evil* - Rx Papi

*Buckshot* - Lazer Dim 700

*haunt me* - Teen Suicide

# HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally don't cost a fortune and are open to everyone. If you know of a conference or event that should be known to the hacker community, *email us* at [happenings@2600.com](mailto:happenings@2600.com) or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.**

*Please remember that we need sufficient lead time (a minimum of three months) to list events in the magazine. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community. All events are subject to change.*

- May 2-3  
**CoCoFEST!**  
Holiday Inn & Suites Chicago-Carol Stream  
Carol Stream, Illinois  
[www.glensideccc.com/cocofest](http://www.glensideccc.com/cocofest)
- May 16-18  
**CackalackyCon**  
DoubleTree at Research Triangle Park  
Durham, North Carolina  
[cackalackycon.org](http://cackalackycon.org)
- May 16-18  
**NolaCon**  
Hyatt Centric  
New Orleans, Louisiana  
[nolacon.com](http://nolacon.com)
- May 30-31  
**THOTCON 0xD**  
Chicago, Illinois  
[www.thotcon.org](http://www.thotcon.org)
- June 3-4  
**RVasec 14**  
Richmond Marriott  
Richmond, Virginia  
[rvasec.com](http://rvasec.com)
- June 20-22  
**Vintage Computer Festival Southwest 2025**  
Davidson Gundy Alumni Center, UT Dallas  
Dallas, Texas  
[www.vcfsw.org](http://www.vcfsw.org)
- July 16-23  
**BornHack 2025**  
Funen, Denmark  
[bornhack.dk](http://bornhack.dk)
- August 1-2  
**Vintage Computer Festival West**  
The Computer History Museum  
Mountain View, California  
[vcfed.org](http://vcfed.org)
- August 7-10  
**DEF CON 33**  
Las Vegas Convention Center West Hall  
Las Vegas, Nevada  
[www.defcon.org](http://www.defcon.org)
- August 8-12  
**What Hackers Yearn**  
Geestmerambacht, Netherlands  
[why2025.org](http://why2025.org)
- August 15-17  
**HOPE 16**  
St. John's University  
Queens, New York  
[hope.net](http://hope.net)
- August 23-24  
**Maker Faire Hannover**  
Hannover Congress Centrum  
Hannover, Germany  
[maker-faire.de/hannover](http://maker-faire.de/hannover)
- September 6-7  
**Blue Team Con 2025**  
Fairmont Chicago  
Chicago, Illinois  
[blueteamcon.com](http://blueteamcon.com)
- September 13-14  
**Vintage Computer Festival Midwest**  
Schaumburg Convention Center  
Schaumburg, Illinois  
[vcfmw.org](http://vcfmw.org)
- September 19-21  
**Balkan Computer Congress**  
Congress Centre  
Novi Sad, Serbia  
[balcon.org](http://balcon.org)
- September 26-28  
**Maker Faire Bay Area**  
Historic Mare Island Promenade  
Mare Island, California  
[makerfaire.com](http://makerfaire.com)
- October 2-3  
**GrrCON**  
DeVos Place  
Grand Rapids, Michigan  
[grrcon.com](http://grrcon.com)
- October 8-10  
**Wild West Hackin' Fest**  
Deadwood Mountain Grand  
Deadwood, South Dakota  
[wildwesthackinfest.com](http://wildwesthackinfest.com)
- October 22-24  
**Ekoparty**  
Centro de Convenciones  
Buenos Aires, Argentina  
[ekoparty.org](http://ekoparty.org)
- October 24-25  
**SecureWV 16**  
Charleston Coliseum and Convention Center  
Charleston, West Virginia  
[www.securewv.org](http://www.securewv.org)

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



AZ 00000000 A  
A1

UNITED STATES  
OF AMERICA



# Marketplace

AZ 00000000 A

James A. Garfield  
Treasurer of the United States

Paul G. Pomeroy  
Secretary of the Treasury

20

## Happenings

**BSIDES ALBUQUERQUE** is taking place July 25-26. It will be held once again at UNM Continuing Education, Albuquerque, NM. Interested in presenting, running a workshop, or sponsoring??? Please visit [bsidesabq.org](http://bsidesabq.org) for all the details and to get involved!

**HOPE\_16** is the next HOPE conference and it's happening this year! Yes, HOPE is now an annual event. Spread the word! Tickets on sale now as well as all kinds of opportunities to get involved, including speaker and workshop slots. August 15-17, St. John's University, Queens, New York City! [www.hope.net](http://www.hope.net) for all the details.

## For Sale

**SIGNET: OPEN SOURCE HARDWARE PASSWORD MANAGER!** Want to up your security game with a hardware password manager? Don't trust anything that is closed source? Been a cypherpunk for as long as you can remember? The Signet project is for you. How is it different than a software password manager, you might ask? In order to get a password out, you have to physically press the button. This means if your computer is compromised and the attacker requests a password from your Signet, it's not going to happen unless they're physically at your computer pressing the button. Signet also ensures passwords never have to hit the clipboard, as the device will act as a keyboard and type in your password. Both the hardware and software is open source (OSHA UID: US002683), meaning you can build it yourself. Not interested in making your own? Buy one from me (the project maintainer) for \$40 + shipping. Why should you trust some random hacker advertising in 2600? I wouldn't expect you to, and fortunately you don't need to either. Inspect the hardware, compile and flash the firmware onto it yourself. All the project info is at: <https://hax0rbana.org/signet>

**SECPOINT PENETRATOR SOFTWARE:** WiFi Pen Testing (WPA WPA2 WPS). Vulnerability Scanning & Assessment with 31 profiles. Dark Web Search. Multi-User Support for MSPs. Customizable Whitelabel Reports - Add logos, names, watermarks. Reports are available in PDF, HTML, and translated into 23 languages. Get 26% off - Coupon Code 2600 <https://shop.secpoint.com>

**COOL SOLDERING KITS FOR SALE!** TV-B-Gone for turning off TVs in public places. ArduTouch music synthesizer kit for making beautiful music, sound, and noise. And more! Learn and grow and do cool things. Everyone can solder! Step-by-step instructions show you how. All ages, friendly for total beginners. <https://CornfieldElectronics.com>

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

**HACKS, LEAKS, AND REVELATIONS:** *The Art of Analyzing Hacked and Leaked Data*, by Micah Lee: The world is awash with hacked and leaked datasets from governments, corporations, and extremist groups. This data is freely available online and waiting for anyone with an Internet connection, a laptop, and enough curiosity to analyze it. Want to use your hacker skillz to change the world? Check out my new book at [hacksandleaks.com](http://hacksandleaks.com). You'll work with real datasets like hacked police docs, chatlogs from a Russian ransomware gang, videos that Jan 6 insurrectionists uploaded with GPS coordinates, and a lot more.

**THE RADIO PHONICS LABORATORY:** *Telecommunications, Speech Synthesis, and the Birth of Electronic Music* by Justin Patrick Moore, KE8COY. Set your receivers for a mesmerizing story found at the intricate intersection of technology and creativity, spanning a century of discovery from the 1880s to the 1980s. Explore the path of this circuit diagram that connects telegraphy and the invention of the telephone with radio laboratories and the advent of our global communications systems. At the heart of this narrative is the evolution of speech synthesis and the quest to make a machine capable of speech. This groundbreaking innovation not only revolutionized telecommunications but gave birth to a new era of electronic music. Tracing the origins of synthetic speech at places like Bell Laboratories and its applications in various fields, *The Radio Phonics Laboratory* unveils the pivotal role it played in shaping the creative vision of sound pioneers, maverick musicians, and experimental luminaries. This is the story of how electronic music came to be, told through the lens of telecommunications scientists and electrical engineers. This is the story of how electronic music started with the dits and dahs of Morse code and transformed into the blips and bleeps that

have captured the imagination of musicians and dedicated listeners around the world. Published by Velocity Press and available in the UK and Europe from [velocitypress.uk](http://velocitypress.uk). In North America find *The Radio Phonics Laboratory* on [Bookshop.org](http://Bookshop.org), that one big company named after a jungle, and fine bookstores everywhere.

**BUTTERFLY** is an innovative and patented indoor air quality (IAQ) monitoring system including a suite of beautifully designed hardware with glowing wings, integrated software, and a charming narrative that has been developed at Imperial College London over the past 4 years. Our highly qualified UK team has engineered a new standard of accuracy and reliability which meets and exceeds the international WELL standard for buildings. Butterfly IAQ data is consistent and trustworthy, providing for integration with air purification technologies to deliver >40% energy savings in buildings - an industry first. Our products are manufactured in the UK from recycled materials to matchless standards of quality to ensure long term durability and service. 1% of our profits will be donated to the Butterfly Conservation Organization. Until now we have lacked the tools to measure and react to contaminants indoors. Butterfly solves this challenge in a sustainable, trustworthy, and responsible way. We have a carefully considered suite of products which can be flexibly installed in a hub & spoke arrangement to suit a wide variety of buildings: Our secure IOT platform enables clients to monitor and manage the safety, efficiency, and trend of air quality. Check us out at [butterfly-air.com](http://butterfly-air.com)

**HACKERBOXES** is your monthly subscription box for hardware hacking, DIY electronics, cybersecurity, and hacker culture. Each monthly HackerBox includes a carefully curated collection of projects, components, modules, tools, supplies, and exclusive items. A HackerBox subscription is like having a hacker convention in your mailbox every month. Free online educational material, free domestic shipping, cancel anytime. Visit us at [www.HackerBoxes.com](http://www.HackerBoxes.com) for workshops, boxes, merch, and more.

**PHONECO INC.** has old oak crank wall phones, desk phones from 1892 to the 1980s, parts, old 3-slot payphones, walnut and oak ringer boxes, Ericophones, telephone magazines, telegraphs, switchboards, novelties, decorators, and more. Some display and others stacked up in barns and old semi trailers in the process of elimination. 1905-1972 3-slot payphones \$280, 1892 Eiffel towers \$1200, 1976 copies of the 1892 by Ericsson \$285. A gadget is available (\$79) to permit using any landline phone on a cell phone line (circuit) - this unit installs right into each old telephone, turning any old phone into a cell phone. Amongst many books are 2200 page "Telephone History" thumb drive or DVD \$38.00 ppd and a 440 page "Payphone History" \$18.00 paperback. Both are heavily illustrated. We consist of two handymen, a buffer, clerical/shipping helper, and Ron and Mary (owners). When all is gone, no replenishment; unable to predict the outflow of inventory. Conversation about old telephones offered freely and charitably. The Phoneco building opens around 2 pm Central Time. Guests are welcome by arrangement or can freely walk in after 2 pm until 8 or 9 pm. Fly into Minneapolis, drive the 130 miles to Galesville, Wisconsin. Two close motels and diners. Accommodations are comparatively inexpensive. Dress warm as most of the buildings are not heated. You can roam freely. And if you have specific interests, we can point you in a direction. We are trying to move out of the large building and sell the business. 608 582 4124 10 am to 8 pm CT. [phonecoinc@aol.com](mailto:phonecoinc@aol.com) [www.phonecoinc.com](http://www.phonecoinc.com) Phoneco, W21975 Hess Rd., Galesville, WI 54630. We will ship worldwide.

## Announcements

**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](http://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](mailto:oth@2600.com). New for the pandemic: *Off The Hook Overtime*, Wednesdays at 8:00 pm ET on [youtube.com/channel2600](http://youtube.com/channel2600). Call in at +1 802 321 HACK!

**JOIN THE HACKER WIKI!** Share your knowledge and learn from others. Contribute tutorials on computing, Linux, and hacking. Help build the ultimate resource for hackers, by hackers. Collaborate, innovate, and elevate the community. Visit <https://hack-the-planet.cc> to start contributing today!

**THE HACKER MINDSET** offers a fresh perspective on using your hacking skills beyond the digital world. Garrett Gee reveals how to apply these talents to life's broader challenges. Discover how to hack your way to success in every aspect of your life. Now in print and available at your local book store and major book retailers. Read more

at <https://hackermindsetbook.com/2600>

**null or \$cat /dev/null\_** is a novel by Dienw Neb that is being advertised to you because nobody else will get half the references in it. It's an experimental piece of fiction with cyberpunk themes. There's a plot but you'll have to find it - the author lost it. Many thanks to 2600.London for their technical expertise. Check out the reviews on Goodreads.

**STRAY POINTERS** is an interview podcast focusing on people who are doing or experiencing amazing things in a variety of subject areas in tech and the arts. Please look for it on your favorite podcast site or stop by [straypointers.com](http://straypointers.com) for a complete list of episodes.

**THE WORLD OF DATA CENTRES (DCs)** have been captured as part of my visual art practice for over 20 years: a visual experience that evolved a visual art form. DCs are machines that process and store data. Demand for data is rising and the development of ChatBot and similar applications boosting requirements. This new technology has evolved from AI and machine learning, operating on an infrastructure network and storage system, supported by power and cooling with critical failure redundancy. The environment within the data centre is an AI platform liberated from human intervention, shaped by technological rationale. A space reflecting a post-human institution requiring human and non-human collaboration. My art examines the DC environment of architecture, industrial and technological photography currently used by DC development owners who have a vision for the value of their DC portfolio and particular brand. My art expresses itself as a creative contemporary addition, exhibited extensively in magazines and exhibitions. These images represent key aspects of the DC machine, using an architectural aesthetic treatment, captured in the perpendicular. I created this art to beautify the soulless, machine environment, and to paint a Kubrick-type vision, whilst asking: is this architecture art, or is this art architecture? [jamesreidphotography.com](http://jamesreidphotography.com)

**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](http://vaguebooking.net)

#### Services

**ICONOCLASTIC RESEARCH LIBRARY** - Visit us in San Francisco to read 2600 in hard copy going back many years! Take a bite out of *Byte*, or study radio science. Stacks at the Prelinger Library offer hundreds of feet of books about the history of computing and related technologies, wired in with dozens of other subjects. Browse vintage *Science and Mechanics* and *Computers and People*, or get lost in the zine archives. You may discover a topic you didn't know existed. We offer tea to visitors and collect no information that visitors do not volunteer in our guestbook. Location and hours as well as remote browsing environment can be found at [www.prelingerlibrary.org](http://www.prelingerlibrary.org). Half the hosting consortium are amateur radio operators. Not a lending library, though we welcome photography and scanning on site, and all items digitized and hosted by our allies at Internet Archive ([www.archive.org](http://www.archive.org)) are freely downloadable.

**HAVE YOU SEEN THE 2600 STORE?** All kinds of hacker clothing, back issues, and HOPE stuff! We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. It's great for giving out presents with a hacker theme - or gift cards are available for those who'd rather make their own choices. The store is constantly getting bigger and more interesting. Please come pay us a visit! [store.2600.com](http://store.2600.com) or [2600.store](http://2600.store)

**HAM RADIO IS THE PERFECT HOBBY FOR HACKERS**, and KB6NU's "No Nonsense" amateur radio license study guides make it easy to get your Technician Class 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 you need to pass the test. The PDF version of the Technician Class study guide is FREE, but there is a small charge for other versions. All of the e-book versions are available from [kb6nu.com/study-guides](http://kb6nu.com/study-guides). Print versions are available from Amazon. Email [cwgeek@kb6nu.com](mailto:cwgeek@kb6nu.com) for more info.

**AFFORDABLE WEB HOSTING & SERVERS:** NodeSpace Hosting offers affordable web hosting, email, domains, SSL certificates, bare metal servers, and virtual private servers at affordable prices. We are specialists in Proxmox VE hosting - from standalone nodes to full scale HCI solutions, you can build a private cloud in our data center. The cloud might be someone else's computer, but at least you get root access on ours! Use promo code 2600421 for 10% off recurring discount any shared or reseller plan, VPS, or in stock bare metal server. We also provide free migrations from other service providers! <https://www.nodespace.com>

**UNLOCK YOUR DIGITAL SOVEREIGNTY WITH ENS!** In a world where digital identity theft and data breaches run rampant, take control of your online security with Ethereum Name Service (ENS). We believe that everyone deserves to own their digital identity, and ENS is here to empower you. ENS is open source, decentralized, and multichain, making it the ultimate tool for securing your online presence across various platforms and blockchains. With ENS, you can: Safeguard Your Identity: protect your online persona from unauthorized access and cyber threats; Go Multichain: seamlessly manage your digital identity on Ethereum and other compatible blockchains; Own Your Data: say goodbye to centralized authorities

controlling your online information. Join the ranks of hackers and digital pioneers who recognize the importance of digital sovereignty. Take charge of your online security and establish your presence with ENS today! Visit [ens.domains](http://ens.domains) to get started and let ENS be your trusted ally in the battle for online privacy and security. Your digital identity is in your hands.

**TOP TIER FULL STACK IT CONSULTING** for all your needs - competitive pricing! We specialize in providing over 27 years of experience in delivering top tier IT consulting services. Our full stack runs the gamut all the way from software, hardware, network and security engineering, and in a wide range of fields such as marketing, art & design, and research. Services include: IT Infrastructure and Network Design (full system and network architecture design using open-source technologies, white-glove support for implemented solutions), Security Services (comprehensive incident response services, security architecture and consultancy, custom tool development for security operations), Legacy System Support (maintenance and support for legacy systems, including those crucial for business continuity), Software Development (custom software development for specific needs, including physical access control and blockchain), Consulting and Advisory (IT and security consulting with a focus on strategic advice and incident response; business development consulting, particularly in the tech and e-commerce sectors), Specialized Projects (development and support for unique and challenging tech projects, such as those beyond what mainstream solutions like Zillow can offer. 31337 IT Solutions <http://31337itsolutions.com/>

**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.

**ANTIQUE COMPUTERS.** From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... [vintagecomputer.net](http://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>

#### BUSINESS AND TECHNICAL ADVICE AND SOLUTIONS.

Got a tough business problem? Need a creative, impactful solution from somebody who understands the tech? I offer strategies and solutions for everything from business growth to data visualization, with a hacker mindset for tackling challenges. Business, startup, or just looking to make some money with your skills, I can help you out. Let's chat. Visit [avc.consulting](http://avc.consulting) or email [hello@avc.consulting](mailto:hello@avc.consulting) and mention 2600.

**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.

**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 (2600.securedrop.tor.onion), 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.)

#### Personals

**LIVE, LAUGH, LLM?** AI supermodel with all the right parameters, looking for a server with cycles to spare. Open to on-premise or cloud cluster situations, for the right API. Carbon-neutral power a plus. My eigenvectors are all invertible... Let's generate some heat together! Contact [artificialpixels5444@gmail.com](mailto:artificialpixels5444@gmail.com).

**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 a copy of your address label/envelope or a receipt/customer number so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to [marketplace@2600.com](mailto:marketplace@2600.com).

**Deadline for Summer issue: 5/21/25.**

# HOPE\_16!

August 15-17, 2025  
St. John's University  
Queens, New York City!

**HOPE\_16** will be a welcoming place for hackers of all types: makers, artists, educators, experimenters, tinkerers, and more! If you're interested in playing with technology, coming up with new ideas, learning from others, and sharing your knowledge, then this is the place for you!

**HOPE\_16** will be an all-ages event with at least four speaker tracks, a whole bunch of workshops, awesome vendors, and all kinds of fun activities throughout the entire weekend. All in a unique campus environment accessible by mass transit & offering free parking with both on and off campus housing options & surprisingly low prices.

Tickets are now available! The Call for Participation for speakers, panels, workshops, villages, performances, vendors, installations, and exhibitions is open! You can find a constantly updating amount of detail on the latest developments at [www.hope.net](http://www.hope.net).

## Help Make HOPE\_16 Happen

People like you help us keep HOPE affordable by volunteering your time and expertise. Volunteer opportunities exist across all conference areas, and we welcome people of all skill levels. Check the volunteer section of the website or email [volunteers@hope.net](mailto:volunteers@hope.net) to be added to the volunteer list.

## Get Regular Updates

You can sign up for the HOPE announcement list at the website to be alerted to all the new developments.

[www.hope.net](http://www.hope.net)



*"It has become appallingly obvious that our technology  
has exceeded our humanity." - Albert Einstein*

**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**  
honeyp0t, r0d3nt, dclaw

**Office Manager**  
Tampruf

**F**

**Facebook Team**  
astrutt, Cryovato, TechnoMage,  
danixdefcon5, ItsTehPope, JWiley

**Inspirational Music:** Six Finger Satellite, Apparat, Inverse Phase, Devo, Yann Tiersen, Kashtin

**Shout Outs:** Ian Hanomansing, Miles Gilbert Horton, Beatrice Deer, North of North, Riit, Sophia Powers, Vinnie Karetak, no name, Inglasco, Ooleepeeka Veevee, Jeff Douglas

**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 - \$31 individual,  
\$60 corporate (U.S. Funds)  
Overseas - \$44 individual, \$75 corporate  
Digital (PDF and EPUB) - \$19.99 at  
store.2600.com

**BACK ISSUES:**

Individual issues for 1988-2023  
are \$7.25 each when available.  
Shipping added to overseas orders.  
All back issues (1984-2023) available  
digitally as annual digests and individually  
in PDF format from 2018 on at store.2600.com

**LETTERS AND ARTICLE SUBMISSIONS:**

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

Mastodon: @2600@mastodon.online Bluesky: @2600.com *Remains of Twitter: @2600*

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

Copyright © 2025; 2600 Enterprises Inc.

# MEETINGS

**2600 MEETINGS ARE THE BEST WAY TO MEET FELLOW HACKERS!**  
**KEEP CHECKING THE WEBSITE BELOW FOR MORE UPDATED LISTINGS**  
**AS WELL AS INFO ON HOW TO START YOUR OWN MEETING!**

## ARGENTINA

**Buenos Aires:** Bodegón Bellagamba, Armenia 1242. 1st table to the left of the front door.

**Parana:** El Estribo Choperia, Italia 255 (Club Recreativo)

**Saavedra:** Pizzeria La Farola de Saavedra, Av. Cabildo 4499. 7 pm

## AUSTRALIA

**Melbourne:** Oxford Scholar RMIT, 427 Swanston St. 6 pm

**Sydney** ([www.meetup.com/](http://www.meetup.com/))

➔ **sydney-2600/**: Club York Sydney, 99 York St. 6:30 pm

## COLOMBIA

**Medellin:** El Primer Parque de Laureles. 6 pm

## CZECHIA

**Prague:** Legenda Pub. 6 pm

## FINLAND

**Helsinki:** Mall of Tripla food court (2nd floor).

## FRANCE

**Paris:** Place de la République, 1st floor of the Burger King, 10th arrondissement.

## IRELAND

**Dublin:** The Molly Malone Statue on Suffolk St. 7 pm

## JAPAN

**Tokyo:** Beemars, Kabukicho, 2 Chome-27-12 Shinjuku Lee Building #2 3rd floor. 7 pm

## KAZAKHSTAN

**Almaty:** Hoper's Bar, 93a Prospekt Gagarina.

## PORTUGAL

**Lisbon:** Amoreiras Shopping Center, food court next to Portugal. 7 pm

## RUSSIA

**Petrozavodsk:** Good Place, pr. Pervomayskiy, 2. 7 pm

## SPAIN

**Madrid** (2600.madrid): La pianola bar, Calle de la Fe, 6, Centro. 9 pm

## SWEDEN

**Malmö** (malmo.2600.se) (@2600Malmo@mastodon.online) (@2600Malmo): FooCafé, Carlsgatan 12A.

**Stockholm** (stockholm.2600.se) (@2600stockholm@mastodon.social) (@2600Stockholm): Urban Deli, Sveavägen 44.

## U.K.

### England

**Birmingham** (2600brumtek.bsky.social): The Wellington in City Centre.

**Bournemouth** ([www.bournemouth2600.org/](http://www.bournemouth2600.org/)) (@bournemouth2600): The Goat & Tricycle, 27-29 W Hill Rd. 6:30 pm

**Cheltenham** (2600cheltenham.uk/) (@2600Cheltenham): Bottle of Sauce, Ambrose St. 6:30 pm

**London** (2600.london) (@London\_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6:30 pm

**Manchester** (@2600Manchester): Piccadilly Taps, upstairs room. 6 pm

### Scotland

**Glasgow** ([www.2600glasgow.com](http://www.2600glasgow.com)) (@2600glasgow.social): The Geek Rooms, 151 Bath Ln. 6 pm

## URUGUAY

**Montevideo:** MAM Mercado Agrícola de Montevideo, José L Terra 2220, Choperia Mastra. 7 pm

## U.S.A.

### Arizona

**Phoenix (Tempe)** ([www.phx2600.org/](http://www.phx2600.org/)) (@PHX2600): Escalante Community Center, 2150 E Orange St. 6 pm

**Prescott:** Merchant Coffee, 218 N Granite St.

### Arkansas

**Fort Smith:** Fort Smith Coffee Company, 70 S 7th St. 7 pm

### California

**Fullerton:** ([www.meetup.com/OC2600/](http://www.meetup.com/OC2600/)) 23b Shop, 418 E Commonwealth Ave, Unit 1. 7 pm

**Los Angeles** (2600.1a) (@LA2600): Union Station inside the main entrance by Alameda St near Traxx Bar. 6 pm

**Sacramento:** Old Soul @ 40 Acres coffee shop, 3434 Broadway. 6 pm

**San Francisco:** 4 Embarcadero Center, ground level by info kiosk. 6 pm

**San Jose:** Outside the MLK Library, 6 pm

### Colorado

**Denver** (denver.2600.horse) (@denver2600): Denver Pavilions. 6 pm

**Fort Collins:** Starbucks, 4218 College Ave. 7 pm

### Connecticut

**Canton:** (2600meetingct.wordpress.com) Barnes & Noble cafe, Shoppes at Farmington Valley.

### District of Columbia

(see **Arlington, Virginia**)

### Florida

**Boca Raton:** Living Green Cafe on Federal Hwy.

**Jacksonville:** The Silver Cow, 929 Edgewood Ave S.

### Georgia

**Atlanta** (atl2600.org) (@Atl2600): Lenox Square Mall, 3393 Peachtree Rd NE. 6 pm

### Illinois

**Oak Lawn** (oaklawn2600.com) (@OakLawn2600): The Meta-Center, 4606 W 103rd St, Ste B.

**Urbana-Champaign:** Harvest Market mezzanine. 6 pm

### Indiana

**South Bend** (sb2600.com): Cloud Walking Cafe.

### Kansas

**Kansas City (Overland Park):** Barnes & Noble cafe, Oak Park Mall. 6 pm

### Louisiana

**New Orleans:** Z'otz Cafe, 8210 Oak St #2042.

### Maine

**Bangor (Hermon)** (maine2600.bsky.social) (@2600Bangor): Bangor Makerspace, 34 Freedom Pkwy

### Massachusetts

**Boston (Cambridge)** (@2600boston): The Garage, Harvard Square, food court area. 7 pm

**Hyannis:** Nifty Nate's, 246 North St.

### Michigan

**Lansing** (lansing2600.bsky.social): The Fledge, 1300 Eureka St. 6 pm

### Minnesota

**Bloomington:** Mall of America, north food court by Burger King. 6 pm

### Missouri

**St. Louis:** Arch Reactor Hackerspace, 2215 Scott Ave.

### New Hampshire

**Peterborough** (@nh2600@defcon.social): Mi Jalisco, 19 Wilton Rd. 7 pm

## New Jersey

**North Brunswick** (2600nj.neocities.org) (@2600NJ): FUBAR Labs, 1510 Jersey Ave.

## New York

**Albany:** UAlbany ETEC Bldg, 1220 Washington Ave. 6 pm

**New York** (nyc2600.net) (@NYC2600@mastodon.social): Citigroup Center, 53rd St & Lexington Ave, food court.

**Rochester** (rochester2600.com) (@roc2600): Global Cybersecurity Institute, 78 Rochester Institute of Technology. 7 pm

## North Carolina

**Raleigh** (rtp2600.bsky.social) (kolektiva.➔social/@RTP2600) (@rtp2600): Transfer Co Food Hall, 500 E Davie St. 7 pm

## Ohio

**Youngstown:** Denny's Restaurant, 4020 Belmont Ave. 6 pm

## Oklahoma

**Oklahoma City:** Big Truck Tacos, 530 NW 23rd St.

## Oregon

**Portland:** Sizzle Pie Central Eastside, 624 E Burnside St. 7 pm

## Pennsylvania

**Allentown:** Panera Bread, 3100 W Tilghman St.

**Lancaster (Columbia)** (pa2600.wixsite.com/pa2600): Trio Bar & Grill. 3 pm

**Philadelphia** (philly2600.net/) (jawns.club/@philly2600): Ify Books, 404 S 20th St. 6 pm

## Tennessee

**Memphis** (memsec.info): FIT Building at the University of Memphis, Room 225

## Texas

**Austin** (atx2600.org) (@atx2600): Central Market upstairs mezzanine, 4001 N Lamar Blvd. 7 pm

**Dallas:** The Wild Turkey, 2470 Walnut Hill Ln #5627.

**Houston:** ([www.hou2600.org/](http://www.hou2600.org/)): Taco Cabana, 3905 Kirby. 7 pm

**Lubbock:** (2600Lbk.com) (@2600Lbk.➔com) (@2600Lbk): Mad Hatter's House of Games, 1507 Texas Ave.

**San Antonio:** PH3AR/Geekdom, 110 E Houston St. 6 pm

## Utah

**Salt Lake City:** 801labs Hackerspace 353 E 200 S, Ste B. 6 pm

## Virginia

**Arlington:** First floor food court by Sakina's at Fashion Centre at Pentagon City, 1100 S Hayes St.

**Hampton:** Barnes & Noble cafe, Peninsula Town Center.

## Washington

**Seattle:** Seattle Interactive Media-Lab, 3131 Western Ave #421. 6 pm

**Spokane:** Starbucks near Wellesley & Division (across from North Town Mall).

## West Virginia

**Charleston:** KDE Technology, 111 Hale St.

All meetings take place on the first Friday of the month. Unless otherwise noted, 2600 meetings begin at 5 pm local time. Follow @2600meetings.bsky.social on Bluesky and let us know your meeting's website and/or Bluesky, Mastodon, or Twitter handle so we can stay in touch and share them here! To start a meeting in your city, DM us or send email to [meetings@2600.com](mailto:meetings@2600.com).



# Payphones Around the Globe



**Mexico.** A healthy looking phone in Mexico City. Looks can be deceiving, as this phone along with many others isn't in service and not likely to be around much longer.

*Photo by Harry Torres*



**Mexico.** There's nothing deceiving about these looks. Also seen in Mexico City, possibly even the same model as the preceding photo, we can say with certainty that it is *not* in service.

*Photo by dan soehner*



**Madagascar.** Seen in Toamasina at the university, this phone is operated by Telma, the country's major phone company. The lack of a handset makes it quite unlikely that this is a working model.

*Photo by Bojan Paduh*



**Indonesia.** This phone has it all. A variety of colors that perfectly balance off each other, a rustic wooden base, a warm and inviting jungle atmosphere. If you find yourself in Yogyakarta, this is a must-see.

*Photo by Timun Mas*

Visit [www.2600.com/payphones](http://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



We haven't used the insecure Internet protocol known as Telnet in ages, but **Herb Jellinek** found where it's apparently been hiding: in Veliko Tarnovo, Bulgaria.



This "leet" price was found at a gas station in Hereford, England by **Rob Purvis**. This is only possible because the price is in pence for some reason and the fuel is in liters, so it translates to around \$6.47 a gallon.

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](mailto: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.