Volume Forty, Number Four
DIGITAL EDITION Winter 2023-2024

2600

The Hacker Quarterly

Taiwanese Payphones

We don't normally print multiple submissions from a single place and rarely from one contributor, but we just had to make an exception after seeing the wide variety of payphones that exist in Taipei. Truly an example for the rest of the world.

This phone with a "Hello Kitty" theme was seen at the Taiwan Taoyuan International Airport.

Here we have a bright yellow phone which was seen around the presidential palace area.

This model was found near the Neihu metro station and has "Epidemic Situation Report" and a whole bunch of directory assistance options on its speed dial listing.

Finally, the bright red option, guaranteed to get your attention. This was also seen by the Neihu metro station. It's pretty much identical to the yellow phone, but the color makes it appear so different.

Photos by Sam Pursglove

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 (Do not send us links as photos must be previously unpublished.)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

Entrées

The Road Behind 4

The Dark Side of DNA Data 6

The BoneBox 9

Artificial Intelligence and Creativity 10

Career and Gloating in Las Vegas 12

TELECOM INFORMER 13

Enhance Your Typing Experience With Mechanical Keyboards 15

Adventures in Lockpicking 17

Ooops; v97.129 18

Geo-Distributed Bug Bounty Hunting 19

Being a Hacker 21

Byte-Sized Justice: A Tale of Hacker Ethics and Copy Protection 23

A Quick Intro to Biohacking 24

HACKER PERSPECTIVE 26

Privacy: Protecting Your Personal Information Online 29

The AI Risk Nobody Seems to Mention 31

American Shanzhai, Part 4 32

LETTERS 34

EFFECTING DIGITAL FREEDOM 46

Quantum Computer Algorithms, Part III: DES Decryption 47

GPT Revolution: Reimagining Programming in the Era of AI 49

Snitched Out by Tech 50

I Fight for the Users 50

ARTIFICIAL INTERRUPTION 52

Platform Capitalism Can't Surveil Absurdism (and Worse) 54

Alzheimer's and AR Tech 59

Book Review: *Pegasus* 60

Book Review: *Fancy Bear Goes Phishing* 60

HACKER HAPPENINGS 61

MARKETPLACE 62

MEETINGS 66

ZW5kZ2FVZQ==

The Road Behind

We've seen some truly extraordinary developments in the world of technology. The theme always seems to be faster, smaller, more revolutionary. As with anything else, a future built on the foundations of the past is one that will survive and grow. But one built on its own without consulting history will inevitably crumble and self-destruct. We see it all the time.

Failure is important in determining what will and won't work moving forward. It makes no sense to keep trying something that has been proven not to work. This goes for everything from technology to legislation. So many poor business decisions are made despite the overwhelming evidence that a particular course of action simply won't succeed. People believe it's somehow different for them, that they've solved the problem, or that those in the past just didn't do it right.

The overwhelming desire for the right to repair is a perfect example of this. It has been proven over and over that consumers want the ability to repair their own vehicles, devices, and property. Yet we repeatedly see attempts to take this away from them, sometimes by even redefining what ownership actually is. In other words, buying a car or a piece of software doesn't mean that you actually own it anymore, but simply that you have licensed it and are subject to whatever terms the manufacturer dictates. While some of us get sucked into this mindset and dutifully pay endless fees for everything from extra speed in our cars to software upgrades that often take away features, there are more of us who fight back and figure out ways around these unfair forms of control.

A key method of losing this battle is to sever links to the past. Forgetting how a certain piece of technology worked back in the day is a surefire way of not understanding its equivalent in the present and the future. If you don't know how it works, you have much less power in determining how it *should* work and how the end user ought to be treated.

Here in the hacker world, we find ourselves in a very strange and unique place. Because of our passion for technology and our almost obsessive desire to learn as much as we can about its inner workings, we find ourselves in a relationship with it that those who simply manufacture or sell technology never get to experience or understand. When the executives upstairs decide to discard hardware or software because of something more profitable, they feel absolutely no allegiance for the old systems or the slightest bit of regret at their loss. They have no passion and they have no understanding. These are two ingredients that hackers have in abundance.

We have heard of so many instances where people are forced into upgrading software and then told they have to upgrade their hardware because their old systems can't support the new software. It seems to be a neverending cycle for many. While upgrades and updates are necessary and important, we seem a bit too eager to abandon something that works in favor of someone else's vision without really knowing why.

We see it all the time with web-based content and social media networks, where people grow accustomed to the way things have been set up, only to be told the rules have changed and all of their content is now in danger of vanishing if they don't accept the new environment. Of course, these companies have the right to do this as these are *their* systems and they can use them as they please. But it's a bad situation for any user to be in when they have relinquished control and must be at the mercy of some faceless entity that they often can't even talk to.

Many of us have fond memories of the old telephone network, a vast sprawling creature that encompassed the world and which we all thought of as an omnipotent entity that would always be there. When we started publishing 40 years ago, the Bell System was in the process of being broken up because it was *too* powerful, and ever since then we've witnessed it change and morph into something else entirely. And that old system that everyone was in awe of back then? It exists mostly in our memories or in telephone museums. The people who run the telecommunications companies have little interest in that. But the hackers and phone phreaks who used to break into those systems of the past are often the ones telling the stories, along with former telecommunications workers like those in

the Telephone Pioneers of America. In the end, it comes down to individuals who love the technology, not the companies that sell it.

Maybe it makes little sense to keep payphones around. After all, everyone has cell phones these days and they cost money to maintain. But while we like technological advances as much as anyone, we know quite well that they don't always work or that new tech is susceptible to things that old tech wasn't. For instance, in a power outage, old-fashioned landlines would still be able to make phone calls for weeks because of the generators at the central office. Today, if the cell tower goes down, you're out of luck. Even those with new fiber optic landlines only have a few hours of backup power available, unlike the old copper lines the phone companies are desperately trying to abandon. Maybe those are conditions we're okay with accepting, but they're definitely a downgrade in that department. We have to wonder if continuing to maintain at least a bare bones network that was more capable of withstanding a sustained outage might not be wise.

Not insignificantly, the purging of old pieces of technology robs us of the opportunity of taking them apart and seeing how they work. That's something you can't really do with the latest, most advanced telecommunications devices. So today's kids don't get to learn that lesson, except maybe through a textbook.

Automobiles are another example of this. For many of us, it's absolutely forbidden to take apart components of your car and replace or upgrade them. You have a shop to bring your car to for that - and not just any shop. Only those licensed by the manufacturer will be supplied with the proper computer codes to access the innards of your vehicle. Any deviation from these rules and you've voided your warranty. In the past, replacing a water pump or changing an oil filter on our own was a rite of passage for many of us. Today we're discouraged from even trying. And we remain ignorant end users as a result.

We may have access to some of the most amazing tech ever invented. But are we truly learning? Is it wise to sunset everything that's old and condemn it to the outdated pile? Can we really understand future technology if we don't understand its history? We don't see how.

Learning to code is a hugely inspirational achievement for many of us. Will we be better off if artificial intelligence can just do that for us? Many experts are saying that's precisely where we're heading. And while it's super cool and awesome to see how quickly AI can whip something together that would have taken us so much longer, we're actually being robbed of the experience and the joy that comes with the process. If simply accomplishing a task and moving on to the next one is all that life is about, then we ought to just sit back and let those tasks get done faster and with less of our involvement. But if life is about building these things ourselves and figuring stuff out on our own, then we ought to stop discarding those experiences in the name of efficiency and start getting our hands as dirty as possible.

Consider what makes a symphony, a painting, or a play a work of art. It's not simply the mathematical arrangement of music, colors, or words. It's the fact that it came from a human mind. That's what ties us to it more than any programmed output ever could. When we give up our hands-on access to anything, we lose that connection that forever ties it to us.

One thing that has never changed throughout every issue we have ever published is the wondrous feeling that whatever has already been invented will pale in comparison to whatever is coming in years ahead. But we should never confuse that inevitability with the belief that everything new is by default better than what came before. Oftentimes, we lose something in the transition - and part of our responsibility is to hold onto that something and preserve it in some way, lest it be lost forever. Visionaries frequently believe that history is something that can be defied because they know better. But that's not how progression works. While we don't need to always be proud of history, we do need to always at least attempt to understand it. In the world of technology, that means tackling the basic concepts that make everything from a steam engine to a mainframe computer operate. When we know how the theories behind the science work and are willing to commit to experimenting on that level, the real learning will quickly follow. Skipping this essential part ensures that we'll become enslaved to a technology we have no understanding of.

The Dark Side of DNA Data: Exploring the Privacy Implications of Aggregated Domestic Genomic Information

by Aniika Gjesvold Cantero

Consumer DNA testing has continued to garner increasing attention in the last decade, and with it has come a stream of promises for research, medicine, and services to consumers. Personalized medicine, cold cases, early disease detection, and family heritage are the main selling points. However, there is an untold side to what is happening with our DNA data as access and ownership shuffle across borders behind the scenes.

At-home DNA tests are relatively straightforward. As an example, Ancestry generates the consumer's results once the saliva sample is processed and run through its proprietary software. According to their privacy policy, they only retain the data if the customer agrees to let their DNA be used for "informed consent research." Additionally stating: "Neither your saliva nor the extracted DNA (together referred to as "Biological Samples") are Personal Information under this Privacy Statement... Future testing may be done if you agree to our Informed Consent for Research or if you consent to other tests of your Biological Samples. If you do not consent to the storage of your Biological Sample, we will destroy your sample."

The saliva sample will be destroyed, but it appears the information extracted from the sample is not. In the case of Ancestry, their DNA "network" contains the DNA information of 22 million people. Advertising, as having the "world's largest consumer DNA network," (Ancestry) further supports the notion that genomic information is being stored long-term and the data is not destroyed unless otherwise requested. According to a recent study, "Vanderbilt University researchers found that 71 percent of companies used consumer information internally for purposes other than providing the results to consumers." (Roberts 2020)

So what's the big deal? DNA data is not like a social security number or other information associated with a person. It is biometric, and an individual *is* identifiable by this information. "DNA presents privacy issues different from those involved in other biometrics collection ... [since] it can contain information about a person's entire genetic make-up, including gender, familial relationships, ... race, health, disease history and predisposition to disease." (Lynch 2012)

Combining personal information with genomic data produces a complete picture of an individual. John Demers, when he was head of the DOJ's national security division, put it clearly when discussing the national security risks of genetic information when he said this data "can be used from a counterintelligence perspective to either coerce you or convince you to help the Chinese," further adding, "the worst case would be the development of some kind of biological weapon ... if you had all of the data of a population, you might be able to see what the population is most vulnerable to" - in addition to the types of exploitation that follow when profiteers gain access to troves of personal information.

Combining genomic information with a complete background check can also identify an individual's closest living relatives and family circle. Once an individual's DNA data is collected, it is not difficult to use today's technologies to identify their closest relatives and family. The NSCS tries to express just how valuable DNA information is, going on to state, "Your DNA is the most valuable thing you own ... It is your unique genetic code and can enable tailored healthcare delivery to you. Losing your DNA is not like losing a credit card ... you cannot replace your DNA. The loss of your DNA not only affects you, but your relatives and, potentially, generations to come."

Direct-to-consumer (DTC) genetic testing data has limited regulations to help protect consumers: "While many companies have robust privacy and informed consent policies, no federal laws prohibit companies from providing individuals' genetic information to third parties." (National Human Genome Research Institute) The Federal Trade Commission can provide some level of protection to consumers by enforcing action if a company makes false claims or misleading statements regarding privacy and security or fails to protect an individual's information. (NHGRI) But in the case of business as usual, DNA data falls through the cracks.

"Ancestry is not a covered entity under the Health Insurance Portability and Accountability Act (HIPAA), and as a result, no data provided by you is subject to or protected by HIPAA." (Ancestry)

Not to say there are no regulations around this type of information at all. Currently, there is a well-defined set of standards issued by the FBI for handling and storing DNA information for inclusion in the Combined DNA Index System (CODIS); the program defines a standard for

support of criminal justice DNA databases and extends to cover the software used to run them. (CODIS and NDIS 2022) However, this is specific to law enforcement and does not cover consumer DNA information generated, stored, and maintained by private companies. (NIST)

Not all privacy policies at these consumer DNA testing companies are the same. For example, 23andMe requires customers to opt in and provide consent before sharing the customer's data. However, this relationship can change if the customer downloads their DNA information and then uploads it to another website. An example of this, provided by Segert, is GEDmatch. GEDmatch's privacy policy is much looser, displays users' real names, and is publicly searchable. The site received infamy when police used it to solve the Golden State Killer case. (Segert)

There are other aspects to this gap, such as when the Genetic Information Nondiscrimination ACT (GINA) was adopted to prevent employers from discriminating against employees based on genetic information. GINA does not, however, apply to third-party direct-to-consumer testing like Ancestry and 23andMe or the handling of the information after it is collected. (Roberts 2020)

De-identifying DNA data, meaning stripping the dataset of personal identifiers, has received skepticism around the accuracy of the claims about the ability to do this successfully. De-identification as a solution to growing privacy concerns is not currently a viable option - "it is not clear if this is entirely effective because genetic data is intrinsically identifying. This is because each person's genome is unique and may be traced back to them similar to a thumbprint." (Segert) In a recent case study, researchers could infer participants' last names using a small portion of their genetic data along with census information such as date of birth and their home state. (Segert) This confirms that it is possible to re-identify an individual after the information has been de-identified.

Additionally, there seem to be lax regulations around a company's ability to sell their customer's genetic information; as Segert explained, direct-to-consumer companies are able to offer their services at an affordable price point because "they can sell their customer's genetic data to pharmaceutical companies for a profit. 23andMe, for example, has a contract to license customer data to the biotech giant Genentech for their research efforts into Parkinson's disease." Relating to 23andMe, it was announced in February 2021 by the Virgin Acquisition Group that the company was being acquired by the firm. (Paul) As the saying commonly goes, follow the money. And in this case, you have to ask yourself what value a DNA testing company geared to learning about your ancestors has to investors like Richard Branson, who are willing to spend 3.5 billion U.S. dollars to acquire it. The answer lies in the asset that a consumer DNA database is and the gap in regulations preventing companies from using and profiting from it.

There also seems to be a deficiency in regulating the limitations of access to U.S. genetic information from foreign entities from a legal perspective. There is currently nothing preventing a foreign company from purchasing a U.S. company that holds DNA data as a primary asset. This has already occurred in at least two documented instances; on December 4th, 2020, it was announced that Blackstone acquired Ancestry for 4.7 billion dollars. Blackstone is a private equity fund with a stake in pharmaceuticals and healthcare-related businesses. Even though Blackstone is an American investment management company, the nature of its partnership structure and the companies they have acquired in the past make them a global entity. (Karr) According to Keith Bradsher of *The New York Times,* the Chinese government holds a three billion dollar nonvoting stake in the Blackstone Group, muddying the clarity of information transfer and ownership around the genetic data we discussed previously.

These are important factors to note when addressing regulatory concerns and determining how the data should be treated. Currently, since this information does not fall under HIPAA, it is covered by regulations that apply to general personal information. More specifically, it is federally regulated based on three criteria: analytical validity, clinical validity, and clinical utility by the Food and Drug Administration (FDA), the Centers for Medicare and Medicaid Services (CMS), and the Federal Trade Commission (FTC) as stated by the National Human Genome Research Institute. These regulations, however, do not regulate or dictate privacy and data handling measures, as well as access and ownership from foreign entities.

There is not a lack of transparency around genomic data, but rather a lack of identifying the data as biometric and handling it with appropriate security and privacy standards, regulations, and procedures. Current measures have failed in their effectiveness in securing DNA testing databases and minimizing the exploitation of the information.

Key takeaways from this effort are understanding the relationship genomic data has with businesses and individuals, and then further understanding what inherent risks emerge. As we have identified, genomic data is

biometric, and there are uses for this information that present threats to U.S. national security and citizens; it is not currently covered under HIPAA, and it is not regulated or prevented from crossing borders or from its purchase by foreign entities.

Countries like China are able to legally purchase genomic data on U.S. citizens with the purchase of companies that possess DNA databases as an asset. Since we have confirmed that the method of de-identification has yet to prove successful, we must also conclude that de-identified DNA data is still sensitive and presents the same risks to national security as the transfer and acquisition of identified DNA data.

It is worth discussing that changes need to be made regarding how DNA data is recognized and handled. It should be first and foremost treated as biometric information that is not strippable of personally identifiable information. Monitoring and restriction should be implemented to prevent the legal and illegal acquisition of U.S. DNA data by China and other adversarial nations that have made their intentions clear that they are not in line with the U.S.'s best interests.

As the value of DNA data grows and more companies place a vested interest, it will get harder to implement regulations and safeguards later. Implementing and enforcing new regulations and frameworks around this information will be challenging, as companies worldwide have already been making multi-billion dollar investments where the access and usage of large DNA databases are the primary assets. Genomic information has been pitched as providing the necessary data to unlock medical breakthroughs that would nonetheless change the future of medicine. Though this is great from a medical research perspective, prioritizing privacy will help ensure that this privacy exists for future generations.

Works Cited

- *2022 Report to Congress of the U.S.-China Economic and Security Review Commission. USCC, Nov 2022,* www.uscc.gov/annual-report/2022-➥annual-report-congress
- *AncestryDNA Informed Consent. (n.d.).* www.➥ancestry.com/dna/lp/informedcons➥ent-v4-en
- *Behind the Scenes: How Does AncestryDNA Work? (n.d.).* www.ancestry.com/cs/dna-➥redirect/ancestry-dna-lab
- Blackstone Inc. (2020, December 4). Blackstone Completes Acquisition of Ancestry®, Leading Online Family History Business, for $4.7 Billion. www.blackstone.com/news/press/➥blackstone-completes-acquisition-➥of-ancestry-leading-online-family-➥history-business-for-4-7-billion/
- *China's Collection of Genomic and Other Healthcare Data From America: Risks to Privacy and U.S. Economic and National Security. The National Counterintelligence and Security Center, Feb.2021,* www.dni.gov/files/NCSC/➥documents/SafeguardingOurFuture/➥NCSC_China_Genomics_Fact_➥Sheet_2021revision20210203.pdf
- *China Says It Made Blackstone Investment to Raise Returns - New York Times. (n.d.).* archive.➥nytimes.com/www.nytimes.com/ref/➥business/22blackstone.html
- *CODIS and NDIS Fact Sheet. (2022, August 3). Federal Bureau of Investigation.* www.fbi.gov/➥how-we-can-help-you/dna-fingerpr➥int-act-of-2005-expungement-policy/➥codis-and-ndis-fact-sheet
- *Company Facts | Ancestry Corporate. (n.d.).* www.ancestry.com/corporate/about-➥ancestry/company-facts
- *Framework for Responsible Sharing of Genomic and Health-Related Data. (n.d.).* www.ga4gh.➥org/genomic-data-toolkit/regulat➥ory-ethics-toolkit/framework-➥for-responsiblesharing-of-geno➥mic-and-health-related-data/
- Karr, R. (2015, February 26). *Understanding the Blackstone Partnership Structure. Market Realist.* marketrealist.com/2015/➥02/understanding-blackstone-part➥nership-structure/
- Lynch, J. 2012. "From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond." Immigration Policy Center: American Immigration Council. papers.ssrn.com/sol3/➥papers.cfm?abstract_id=2134481
- NHGRI. (2019, March 13). *Regulation of Genetic Tests.* www.genome.gov/about-➥genomics/policy-issues/Regulat➥ion-of-Genetic-Tests
- NIST. www.cstl.nist.gov/strbase/➥QAS/Final-FBI-Director-Databasing-➥Standards.pdf
- Paul, K. (2021, February 11). *Fears Over DNA Privacy as 23andMe Plans to Go Public in Deal With Richard Branson. The Guardian.* www.theguardian.➥com/technology/2021/feb/09/23andme-➥dna-privacy-richard-branson-➥genetics
- *Privacy Statement. (n.d.).* www.ancestry.com/c/➥legal/privacystatement
- *Privacy in Genomics. (n.d.).* www.geno➥me.gov/about-genomics/policy-➥issues/Privacy
- Roberts, B. C. (2020, July 23). *Your Genetic Data Isn't Safe. Consumer Reports.* www.➥consumerreports.org/health-➥privacy/your-genetic-data-isnt-➥safe-direct-to-consumergenetic-➥testing-a1009742549/
- Segert, Julian. (2018, November 28). *Understanding Ownership and Privacy of Genetic Data. "Science in the News."* sitn.hms.harvard.edu/➥flash/2018/understanding-ownership-➥privacy-genetic-data/

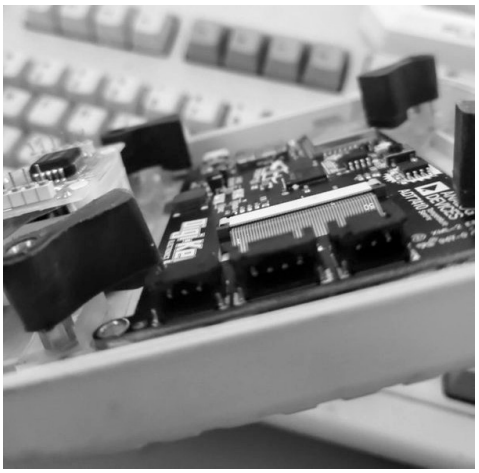
The BoneBox

by Delchi

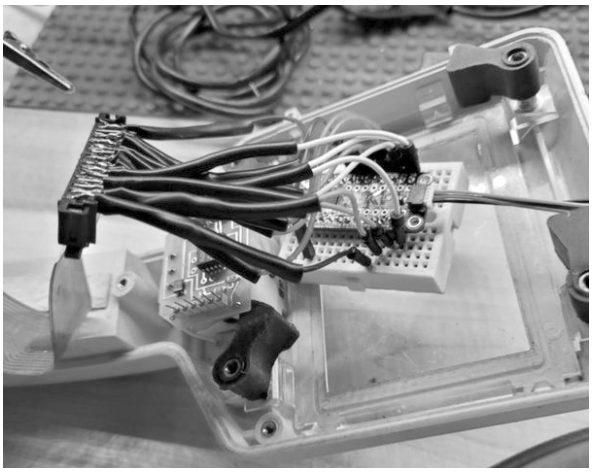
Phreakers have long cherished the lineman's set, also known as a "butt-set" or a beige box for connecting to phone lines. A staple tool of the phone technician and telecom worker, they remain both a useful tool and a collector's item in the age of VoIP. A variant of the lineman's set was known as a "Craft Access Terminal" (CAT) or a "dogbone," so called for its large size and the shape of a dog toy bone. This was a combination of lineman's set, a modem, a joystick and an LCD display screen. It was featured in *Phrack Magazine* Volume Seven Issue 48.

The purpose of the CAT was to allow the person working on the line to access the switch to expedite deployment of phone lines instead of calling and waiting for provisioning. This made it a must-have tool for phreakers who could lay their hands on one, who would try to find the passcode to the switch, which was not always a tricky thing to do. In the late 90s, a switch in Brooklyn had the passcode 000000.

So here I am in 2023 and in my boxes of gear I came across an old AT&T branded dogbone that I bought at a tech flea market. The battery was long since dead, and it did not respond well to being used as a lineman's set. The switches that were designed to interface with it are long gone. I was about to retire it as a museum piece to collect dust for all time when I had an idea. Recently I had read an article about the Adafruit PyPortal - an all-in-one computer with a touch screen color display - and the things it could do with Python. Like Bernie S. with a handful of crystals, I knew what had to be done. Thus, the BoneBox was born.



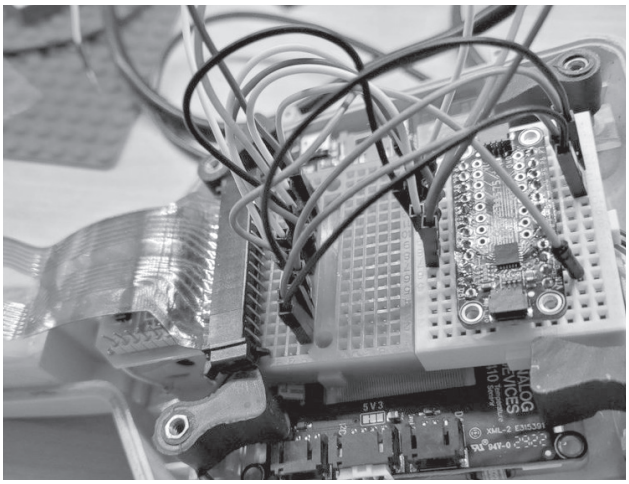
A few screws loosened later, I discovered that the PyPortal is very nearly the exact size of the LCD display in the CAT. Likewise, the keypad was a standard 3x4 DTMF touchpad with a single line to each button. The ribbon cable connecting it all together was aged and delicate but serviceable. I was able to strip out the LCD screen, modem, and the brains of the CAT and desolder the connector that connected the touchpad to the brains.



It was then that I ran into the first snag: the PyPortal did not have enough GPIO pins in order to service the entire touchpad. I added a GPIO expander board on a small breadboard and then soldered each pin, each protected with a heat shrink tube, from the original connector to the GPIO expander board. Some quick test code in Python and I was able to recognize all the buttons on the touchpad.

The next challenge was to supply power to the PyPortal. On the side of the dogbone there is a sliding mode select switch which I removed, leaving the cap of the sliding selector in place.

I then used a dremel to remove some of the plastic, exposing the USB power connector of the PyPortal, with the added bonus of the sliding selector acting as a cover when not in use. Next I used an Adafruit power and charging board along with a new lithium ion battery that fit in the battery compartment to make it portable. Thanks to some old school hacking, wiring skillz, and creativity it all fit together and I had a working touch screen interface with a DTMF keypad.



The next question became what to do with it all. A blue box? A red box? The honest answer was "Why not both?" After acquiring the needed tones from the Internet, I had everything I needed to code up a touch screen interface to allow me to use the dogbone as a red box, blue box, and to create the 2600 hertz tone of days gone by. The dialpad was lacking the A, B, C, and D buttons, but some quick coding and I had added those buttons to the touch screen interface. Still, something was missing. This was a complete throwback to the golden age of phreaking, but it lacked anything truly modern. I then recalled that the PyPortal has a full complement of Wi-Fi on board, so with some tinkering around the limited memory and practicality I added a Wi-Fi access point scanner to the arsenal. I now had transformed an ancient piece of days-gone-by technology into a conversation piece and tool for the ages. I'll be clipping it on my belt and taking it to DEF CON to show that I truly put the old in old school.

Parts List

- One Dogbone
- Adafruit PyPortal (part #4116)
- Adafruit Powerboost 1000C (part # 2465)
- Adafruit lithium-ion 3.7v battery (part # 1781)

Delchi is a long time denizen of the hacking/phreaking scene. He is the inventor of the Spider Box HID card hacking tool (H2K2) and Rolling Thunder, a power wheelchair pen testing platform. In the past he has been a volunteer at the HOPE convention, guest on Off The Hook, *member of The Dorsai Embassy hackerspace, DJ and roadie to the hacking community, and currently is the lead of HDA (Hackers With Disabilities) at DEF CON as well as a five-year veteran goon. Shai Dorsai!*

Artificial Intelligence and Creativity

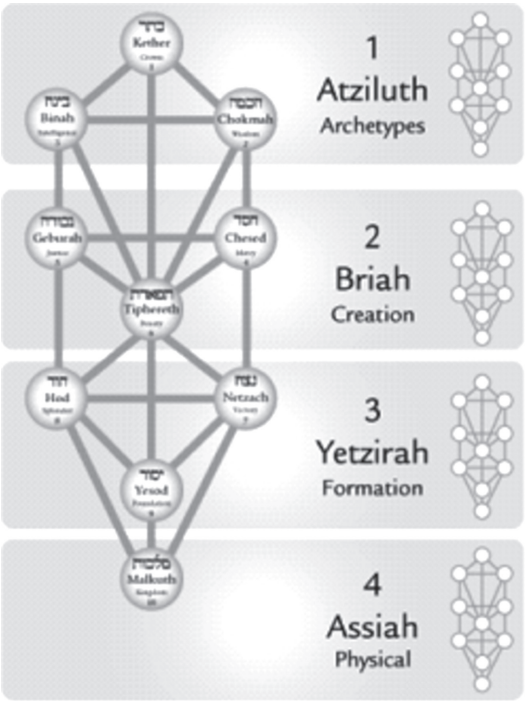
by Ben Belinsky

The biggest challenge that artificial intelligence (AI) presents to many people is its encroachment on the human preserve of creativity. It touches the sense of ourselves as creators. We give ourselves the name Homo Sapiens, meaning "Man the Knower." Also, Homo Faber, "Man the Maker." But behind them all is Homo Creator, "Man the Creator." We do not grant any other being in the world this status. We are created but we are also creators, something we claim to share with the gods. All other beings are mere creatures.

But there's creating and creating, and to understand the differences we turn to the ancient philosophical and metaphysical tradition of Kabbalah, which describes the process of creation.

According to Kabbalah, there are four different worlds, each with its own level of creativity.

Reading from the bottom up:



Assiah

This name comes from the verb "to do" in Hebrew. It refers to action. I open a door and enter a room. These are actions, but I have not created anything.

Yetzirah

This name comes from the verb "to form" in Hebrew. The noun relates to pottery - taking the clay and forming it into a pot.

Beriah

This name comes from the Hebrew verb "to create." It's the verb that's used in the first line of Genesis: "In the beginning God created the heaven and the earth." It refers to creating something out of nothing - similar to the way that virtual particles are said to pop in and out of existence at the quantum level.

Atziluth

This does not come from a verb. Rather, it comes from a preposition for which there is no translation in English. French has the word "chez" as in "chez moi" - at my place. In German it's "bei" as in "bei mir" with the same meaning. Here, Atziluth is the noun formed from a preposition which has the sense of being at someone's place; in this context, the place of the gods: "Chez les dieux" in French, or "Bei den Göttern" in German. "At the gods" would be the translation into English.

So when we look at the process of creation, we read from the top with Atziluth, the world of archetypes and Platonic forms; the world the divine concepts; the four-dimensional forms from which our 3D world is cast. This is the world of the gods and we have no business there. Then we step down to Beriah, the word of God that creates the world. Then to Yetzirah, how the pieces of the world fit together, how they combine and separate, forming physical reality in its ever-changing flux. Then down to the basic level of doing with Assiah, the actions that take place in physical reality that sanctify or profane that reality.

Artificial intelligence can operate at the level of Assiah: doing. It can switch on or off a light, it can order milk if you're running out. AI can also operate at the level of Yetzirah, taking the bits and pieces of the world and putting them together in different ways, like an engineer or bricoleur, scouring the Internet to write, say, a tourist guide to Vienna or a recipe for Sachertorte.

But can AI operate at the level of Beriah? In the Greek language, this word can be approximated by the word poiesis - "the activity in which a person brings something into being that did not exist before." This is the process of making a poem or a song. Sure, a poem is a collection of pre-existing units (words) and can therefore be seen as formed (Yetzirah) in the way a potter forms clay to make a pot, or the way wood is mashed up to make paper. Sure, the words create meaning which is greater than the sum of its parts but it's still Yetzirah. From this point of view there's still no essential difference between this sentence and a poem. They are both created from strings of words which are in turn created from strings of letters which evolved from ancient picture writing.

What makes the difference is poiesis, the process that can only happen in the world of Beriah. This was described by the German philosopher, Martin Heidegger as "bringing forth." For gods this is easy. They just say the words and it is so. For humans, the nearest we get to it is in the making of a poem. A poet has a flash of inspiration which can be described as a bringing forth from the fire of lived experience. We use words like "magical" to describe it because it is so beyond our everyday worlds of Assiah (doing) and Yetzirah (forming). This is the quality that distinguishes Beriah.

And this is something that AI cannot do and may never be able to do. No matter how technically proficient an AI program may be, no matter how many poems or songs it may ingest and analyze, what is shat out or spat out lacks this quality of poiesis, of true creation. So, for the moment, AI must remain as a tool and Homo Creator is safe from the predations of the machine world.

WRITERS NEEDED

Send your articles on hacking & technology to articles@2600.com

Career and Gloating in Las Vegas

by Thrunter X. Thoompson

We were on the edge on Luxor when the thought leadership began to take hold... I found myself in possession of a Blackhat yellow badge. This meant I was restricted to the revenue generator known as the vendor floor where I would see nothing but free t-shirts, charging cables that I'll never plug a device into, and industry luminaries imploring me to zero-trust this, and AI that.... The AI is everywhere, slowly devouring entire functional teams with its undeniable allure of free work generated by the lying plagiarism machine. All I could think of was the banality of future endeavor, and where my next drink was coming from.

As I roamed the endless wasteland of disposable tchotchkes and near future car washing rags, all I could see were entire corporations built to service a dying paradigm. Selling complex tools to provide a feeling of comfort to lure these poor reptiles into a quiet complacency that their misconfigured tools would make them safer for the low low prices of whatever it takes to hit my revenue goals. This is not a place of honor, but of honorifics... an entire industry built on becoming superhuman, a force-multiplier, an all-knowing beast, hell-bent on controlling the flow and availability of information all in the name of safety. In some cases, it succeeded at that goal, but then iterations were seen, different groups doing the same thing as the other with different branding... New clothes for every tiny Caesar in the room.

The opportunity to talk about your accomplishments and brag to others about what you've done in the past year while they only half listen because the alcohol-drenched souls in the room can't conceive of any information that doesn't shore up their own secretly fragile egos, is everywhere and taken at every opportunity like some sort of terrible antidepressant that just leaves you sadder. I had been in Vegas for four days by the time this orgy of security by finance committee had started and had already become an animal. This city will do that to you: tear you down and transform you into an automaton of indulgence in a human suit, and that makes for a surreal experience at the corpo version of DefCon. Walking among them in my human suit, not trying to say the quiet part out loud... infosec was a mistake.

The juxtaposition of shilling well-crafted combinations of existing open source tools combined into a platform that is a glorified workflow organizer is a time-honored tradition in this industry, full well on display at BlackHat. A black mirror of the capitalist hellscape, finding ways to generate value from the work of others who will never be compensated for their willingness to work selflessly to make the world better. An exploit that will never receive a CVE, nor a patch. These poor rubes don't even know they are being taken advantage of, and by the time they do there is a steady stream of others hungering for the approval of their peers, like a gifted kid waiting to be picked for a kickball team. We embrace this model in the name of efficaciousness and modernity, but we need to recognize it for what it is, an exploitative labor model taken advantage of by nearly every software vendor in the world, not just infosec.

We all want to make the world better, but don't you dare ask for compensation for the work that enables a corporation to defend its assets - who do you think you are anyway? You don't have the lawyers nor the standing to even ask for compensation for the tools they rightfully colonized. "Get back into the codemines!" they'd shout at you... and you would, because that's what we do... we must create. Are we not humans with extraordinary knowledge, whether gifted or learned through labor?

Were it not for the work of the counterculture in this field, the hackers that are so often maligned, would this industry even exist? This whole Jenga Tower came to be because of fear and media influence exerted by those same kids waiting to get picked for the kickball team, but they found the secret hideout and worked from there, in the alley out back, in the treehouse, like a cyberpunk version of *The Little Rascals*. Were it not for their nudges to corporate giants in the 90s and early aughts, would we have compliance and regulatory governance? Certainly not in any sort of fashion that would allow for the density and excess that is on display in the desert at BlackHat. Those hackers may draw a paycheck from infosec now; we all have mouths to feed, bills to pay, and those forces work real well as a clothespin on the nose to try to ignore the smell. But that odor of misguided hubris and capitalistic masturbation still clings to everything we do.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It's winter, which means power interruptions here in the Great Northwest. Most of our power (and telephone) lines are above ground, and the whole region is covered with trees that average over 100 feet tall. Trees and branches are falling constantly causing power interruptions, especially during the fall and winter. It has been getting worse in recent years, though, given that summer weather keeps getting hotter and the rainy season is ever shorter. Making matters worse, we have been getting more "atmospheric rivers" as of late, which deliver several inches of soaking rain at a time, saturating the ground. When a windstorm happens after this, large trees like cedars with shallow root systems simply blow over. They fall onto cars, houses, and (of course) power lines. I'll give you one guess whose power line was taken out by a tree today. If you guessed a central office with "Forest" in the name, you'd be right. I'm acting in an incident response capacity today, dealing with possibly the strangest incident that I have ever experienced in my career. But we'll get deeper into that later. For now, let's talk about power engineering.

Obviously, downed trees and power interruptions are nothing new in the Pacific Northwest, and we have been prepared for them for a long time - including in the central office where I am working today. Now, you probably don't think of the USDA as a telecommunications regulator (the FCC writes most of the rules), but they have made a significant mark on the telecommunications landscape. I doubt that the company would have been so well prepared for emergencies if it wasn't contractually required!

If you're scratching your head, I'll explain. The USDA, through the Rural Electrification Administration, provides subsidized financing to telephone companies. These subsidies were intended to serve rural areas, but as the population of the Pacific Northwest grew, the Company was very effective in its lobbying to secure financing for suburban and exurban locations in its service territory. This saved hundreds of millions of dollars in interest, which could instead be used to buy back shares of company stock and help executives meet their bonus targets.

In a rare case of CEO incentives aligning with public good, the USDA loan program has underwriting requirements which enforce minimum central office construction standards. In fact, they publish an entire reference engineering guide, and this includes power supply and backup power requirements. With peak loads assumed, the USDA requires either eight hours of backup battery power or three hours of battery power plus a diesel generator. In 2007, the FCC eventually weighed in after Hurricane Katrina with Order 07-177, releasing a loophole-ridden, watered down rule applying to all telecommunications facilities (not just ones funded by the USDA). It was then immediately challenged in court.

This particular central office is equipped with a three-hour backup battery system and a diesel backup generator. One room on the ground floor of the central office is dedicated to our backup battery system, and the generator is located outdoors. Both systems are required to provide enough power to run the central office during peak load, and do so effectively. There are varying requirements on how much of a fuel supply we need, but this central office was constructed in 1982, not long after the Mount St. Helens eruption (which happened in 1980). This was obviously fresh in the minds of the engineers who designed subsequent central offices. Without knowing what regulations might be forthcoming, they provisioned 72 hours of peak load fuel storage on-site. In practice, we have about five days of fuel, because the central office doesn't run at peak load at all anymore, and especially doesn't do so for 24 hours per day. As with our backup battery contract, we have a fuel services and maintenance contract with an outside vendor.

This all sounds great, right? It's all good in theory. It's also good in practice: this stuff is regularly used! We have weather events *all the time* during Pacific Northwest winters. Most of the problems I'd normally encounter would result from deferred maintenance or a component failing. This time, though, a tree is down, we don't have utility power, and the clock is ticking. You see, our compliance department abruptly ended our contracts with our fuel service vendor who also happens to be *the only fuel depot in the region*. The fuel depot doesn't know why, Compliance wouldn't tell me why, and it finally took a Washington Utilities and Transportation Commission rule to prompt a solution.

I showed up three days in while we were running on backup power. A landslide had

taken out our utility feed to the central office, road access to the utility lines, and several utility poles along with it. Although some of our outside plant was impacted, we were lucky: we only had a few subscribers in that direction. Our power was out, though, and it was going to be out for a while - at least two more days. This wouldn't normally be a problem; after all, we are well prepared with backup power and the central office itself was accessible via other routes. When I arrived, we had about a third of our fuel remaining for the backup generator, and a battery backup operating with a failed (but redundant) PDU. Normally, none of this would be a big deal. PDU failures happen, especially when switching over to generator power, which is why we have redundant ones. We'd want to fix it before we switched back to utility power (in case the same thing happened again with the switchover), but that was manageable. Fuel is normally no problem, since roads were open and critical utilities like telephone service have priority on constrained supplies (which, in this case, weren't even constrained). We just needed to call the fuel depot for delivery, and call our electrical vendor to fix the PDU.

This is all easy stuff - well, not *easy,* but manageable. We have a standard operating procedure for it. All of the contracts are in place. Should be a cake walk, right? That's what I thought, until I called the fuel depot. "No truck. You guys terminated our contract!" said my contact at the fuel depot. "What? That doesn't make any sense. I'll get with the contract guys, but in the meantime, can I get the truck out? We're running pretty low," I said, my jaw almost hitting the floor. "Not a chance," said my contact at the fuel depot. "Cash up front is the only way we can do business without a contract on file, and *you guys terminated the contract*. Send us a wire, and we'll deliver fuel. Here are the wire instructions...."

Obviously, I didn't have the ability to wire thousands of dollars of company money to buy fuel, so I called Accounts Payable. They could pay an invoice, but it needed a purchase order. That was the responsibility of Procurement. I contacted Procurement, and they couldn't issue a purchase order without a contract. They referred me to Contracting. Contracting notified me that they couldn't issue a contract because they had terminated the contract at the instruction of Compliance. They suggested I talk to Compliance. I called Compliance and left a message, marking it as urgent. In our voicemail back-end system, I could see that Compliance had 143 other urgent voice messages, so I was guessing this might take a while. OK, fine. Time to notify Compliance Legal. In the state of Washington, we're required to notify the Utilities and Transportation Commission of critical utility outages, with an explanation as to what caused them. I left a voicemail for Compliance Legal letting them know that I would be filing a major outage report with the UTC if I didn't hear back from them.

Well, that set off a firestorm. Compliance Legal called me back, and fast! They absolutely did not want me to file an outage report. Could I do anything to prevent this? "Yes. Help me get some fuel," I said. "Our fuel service contract was canceled by your department. I have no idea why." Now, as it turns out, people in Compliance pick up the phone when it's their own legal team calling. The next morning, with only 15 percent fuel remaining, I was finally able to arrange fuel delivery and find out what happened (we paid up front just like the fuel depot asked).

Our fuel services vendor has the same name as a different fuel services company in Malta. It's not the same company, isn't run by the same people, and has nothing to do with them. However, there is also an obscure division of the Department of the Treasury called the Office of Foreign Assets Control, aka OFAC. They enforce financial sanctions using a watchlist - you know, sort of like the TSA no-fly list and various terrorist watchlists. The OFAC list used to have a few obvious terrorists and terrorist organizations on it, along with countries sanctioned by the U.S. (think Iran, North Korea, Cuba, etc.). These days, it's a 13.4 megabyte file with thousands of names (including Mike. Just "Mike." Sorry if your name is Mike.). And as you have probably guessed, a sound-alike Maltese fuel services company is on the OFAC block list. Now, if anyone involved in this had any common sense at all, they would have investigated a bit more before cutting off my fuel supply. But this is the corporate office we're talking about, and they bought an AI tool to ensure compliance. So, compliance with an outage report was nearly ensured.

And with that, enjoy your winter. For my part, I still haven't figured out why our PDU tech hasn't arrived.

References

- USDA Rural Electrification Administration Power Requirements For Digital Central Office Equipment: `www.rd.usda.gov/files/➥UTP_Bulletins_1751E-302.pdf`
- FCC Order 07-177 (Hurricane Katrina Commission): `docs.fcc.gov/public/➥attachments/FCC-07-177A1.pdf`
- Washington Utilities and Transportation Commission Outage Reporting: `www.utc.➥wa.gov/regulated-industries/➥utilities/telecommunications/➥telecom-reporting-requirements/➥telephone-outage-reports`
- OFAC Specially Designated Entity list: `www.➥treasury.gov/ofac/downloads/➥sdnlist.txt`
- What to do if your credit report is OFAC flagged: `ofac.treasury.gov/faqs/topic/1516`

Enhance Your Typing Experience With Mechanical Keyboards

by writerbenjamin

Older geeks remember the sound of typing on an IBM model and how the cheaper rubber domes that later replaced them just aren't as pleasurable to type upon. However, mechanical keyboards, especially with the Cherry switch technology are revolutionizing computer input. This article is meant to introduce you to the basics of mechanical keyboards.

So how are mechanical keyboards different from the keyboard that came with my computer? What is the difference between tactile, linear, and clicky switches? What are doubleshot, laser etched, or pad pressed keycaps? Is RGB lighting even necessary? And is that different from red, blue, green, brown, or black switches? I'll attempt to explain this here. (Please note that building mechanical keyboards is beyond the scope of this article.)

The keyboard that came with your computer is usually a membrane keyboard, otherwise known as a rubber dome. The difference is in how the keys are actuated. In the membrane keyboard, the switches consist of a rubber mat that covers the entire circuit board of the keyboard. There is a rubber dome under each key which contains a round carbon disk. The printed circuit board has the keyboard matrix with contact for each key. When the key is pressed, it pushes the carbon disk down onto the contact and sends the computer the key code for the key that was pressed. This gives a mushy feel and the key must be pressed all the way to the bottom of the key's travel to activate.

Mechanical keyboards are keyboards where each key is a physical switch. These switches are soldered directly onto a printed circuit board. The switches usually contain a spring, a stem, and a plastic housing. Metal contacts inside the switch are shaped in such a way to give different properties to the switches. The keycap connects to the stem on the switch and the stem presses against a spring in the housing. Inside the housing are the metal contacts. The stem presses the contacts together at a specific point in its travel. This becomes important later in the section on types of switches. Once the switch activates, it sends a key code to the computer.

What are the advantages of mechanical keyboards? First, the typist need not bottom out the key to actuate a key stroke. Instead, the key actuates somewhere in the middle before the key reaches the bottom of its travel. By not pressing the key all the way to the bottom of key travel, this reduces repetitive strain injuries while typing. Additionally, the key's switches can be configured for stiffer and lighter resistance or to provide feedback when the key actuates.

There are three modes of mechanical keyboard actuation: linear, tactile, and clicky. Linear switches actuate consistently through key travel.. For example, as the typist presses a key, it requires more and more force to continue pressing the key. There is no feedback when the key actuates, but they are faster and have a smooth regular travel when the key is pressed. This trait is prized by gamers, as many believe it increases performance where accuracy and precision are necessary. Linear switches are very quiet as well, as long as you don't bottom out the key travel.

Tactile switches, on the other hand, do not have a linear feel. Instead, when they are pressed, there is a slightly heavier feel just as the key actuates. These switches are not as quiet as linear switches, but the typist gets feedback at the actuation point so they know when to stop depressing a key. This trait is useful for writing or typing. This is also quieter than the next category, the clicky switch.

Clicky switches are more controversial among mechanical keyboard users. Clicky switches are tactile switches which emit an audible click when the switch is actuated. This gives the user more feedback than with a tactile keyboard, as it gives off a sound as well as the tactile bump. The reason it is controversial is the switches are loud. Other people might be annoyed by the sound. However, it is the best for a typing situation, depending on preference for the audio experience. It can become a problem when the sounds of keys typing might be picked up on Skype calls or when recording podcasts.

Mechanical keyboards are categorized by size. Full size keyboards have 104 keys and have a top row with function keys, an area with arrow and navigation keys, and a numerical keypad. The numerical keypad duplicates the number row at the top of the keyboard as well as the arrow and navigation cluster and can be toggled between modes with the Num Lock key. The next smallest keyboard size is a tenkeyless or 87 percent keyboard. This keyboard simply doesn't have a numerical keypad. This maintains a standard keyboard layout, but allows the user

to hold the mouse closer to the keyboard. The 60 percent keyboard only has the letter and number keys. The function keys are omitted along with the arrow and navigation keys. There is also a variant of the 60 percent called the 65 percent keyboard which has an extra column of keys on the right side which are usually used as arrow keys or navigation keys. The smallest keyboard you can type on is the 40 percent keyboard. This keyboard also omits the number rows from the top of the keyboard. Usually there is a function key to access the missing keys on lower layers of the keyboard. The final keyboard type is the numpad. This keyboard is only the numerical keypad, which is useful when you have a tenkeyless keyboard and sometimes need to work with numbers or spreadsheets.

Mechanical keyboard switches are also measured by actuation force. This can be adjusted by installing weaker or stronger springs. Thus, the switches can be classified by activation force and type. The default color scheme is the Cherry MX color scheme where red and black are various strengths of linear switches, brown and clear are various strengths of tactile, and blue and green are variations of clicky switches. The reds, browns, and blues require about 45 grams of force to actuate. The blacks, clears, and greens require about 60 grams to actuate. The color schemes of the switches are only present in the stems of the switches and the purpose is to show the type of switches. The color schemes vary by manufacturer, as there are many clone switches that aren't made by Cherry. Some of the switches from other manufacturers are better than the Cherry style switches.

This is not to be confused with the colors of the LED lights on RGB keyboards. RGB lighting allows the keyboard to light up in various colors and patterns. Not all mechanical keyboards have LED lighting - some have only a single color of LEDs, but others have multicolored LEDs that can be changed programmatically. These RGB lights can show patterns such as solid colors, breathing, the wave, and star burst. RGB lighting is primarily on mechanical keyboards marketed toward gamers.

Keycaps are the top part of the key which have the letters written on them. These are for customization, provided your mechanical keyboard has Cherry-style switches, which most do. The keycaps can be bought separately and come in different colors or themes. Cherry style key caps are categorized by the shape of the keycap, the type of material used, and the method by which the characters are affixed to the key.

There are four main ways to affix the character symbol or lettering on the key. The easiest and cheapest method is pad printing. These are made by pressing pigment onto the key with a pad press. The disadvantage is that the lettering can rub off over time. Another method is to laser etch the keys. The keycap is painted and a laser is used to etch the letters into the keycap. These are also cheaper and prone to wear. The third method is dye sublimation. The plastic of the keycap has lettering dyed into the surface of the plastic. The disadvantage of this method is that the letters have to be a darker color than the keycap. This limits the colors that you can have on a dye sublimated keyboard. The final method is the double-shot keycap. In this method, the lettering and the rest of the keycap are injection molded and then pressed together. No matter how worn the keycaps get with use, the lettering will stay bright and legible.

Keycaps are made out of two main types of materials: ABS or PBT. ABS keycaps are made of the same material as Lego bricks. They are injection molded and they tend to be very smooth. The main disadvantage is that the user will polish them into a shine as they are typing. Among gamers, this shine will show up first on the WASD keys. However, you can buy higher quality ABS keys that don't develop a shine as quickly. The advantage of ABS is you can get a better variety of keycaps. Some mechanical keyboard users don't like the shine and prefer PBT keycaps. These keycaps are made from a harder plastic than ABS. They are more durable and have a textured surface that doesn't develop a shiny surface over time.

The final category of keycaps is the shape of the keys. The most common shape of keys is the Cherry or OEM keys. The main difference is OEM keycaps are slightly taller than Cherry keycaps. Both these keycap styles are middle of the road for keycaps. The keycaps are taller at the tops and bottoms of the keyboard and shorter at the home row which makes reaching for the keys easier. DSA keycaps are a uniform shape and height on every key on the keyboard. These are shorter than Cherry and OEM style keys. SA and MT3 keycaps are very tall sculpted keycaps. They are even taller at the higher rows on the keyboard and are slightly smaller on the home row. These are never the keycaps that come stock on a keyboard and they must always be purchased separately.

This should cover the basics of the idea of mechanical keyboards and give you enough information if you wish to shop for or just understand mechanical keyboards.

Adventures in Lockpicking

by Street

I was initially introduced to *2600 Magazine* through locksport, a hobby that involves recreational lockpicking and exploration of physical security systems. It was through this community that I discovered the intriguing world of hacking. The adage "you own a machine as soon as you have physical access to it" resonated deeply with me, and my own experiences have proven its validity. Armed with a boot disk I obtained from Lazesoft, I possess the ability to bypass any Windows login and gain unrestricted access to almost anyone's home computer. This newfound power fueled my curiosity and desire to delve deeper into the world of cybersecurity. I plan to attend the HOPE conference in the near future, where I can meet more people who share these interests. I am particularly eager to see TOOOL (The Open Organization of Lockpickers).

Lockpicking and hacking share a fundamental connection rooted in the exploration of security systems. Surprisingly, locks are often the weakest link, even in computer security systems. Most buildings have locks from one of two prominent manufacturers: Kwikset and Schlage. These two brands dominate the market, accounting for approximately 90 percent of the locks and keys used in doorways. While there are other lock manufacturers in the industry, many of them produce locks with the same keyways as Kwikset (and sometimes Schlage).

A simple Google search reveals the most commonly used keys for these popular locks:

Kwikset KW1: This key, designed for 5-pin locks, is manufactured by Kwikset and other companies. It is the most common choice for residential homes.

- Kwikset KW5: Serving as a 6-pin version of the KW1, this key offers enhanced security and is also produced by various manufacturers.
- Schlage SC1: Widely utilized in residential locks, the SC1 key is designed for 5-pin locks.
- Schlage SC4: This 6-pin lock is commonly found in commercial doorways and provides an extra layer of security.

For those interested in these specific types of locks, Original Lishi (www.originallishi.com) offers an innovative solution. The company has developed a line of lockpicking tools that operate almost automatically, revolutionizing the locksmithing process. Having personally used these tools, I can vouch for their reliability and effectiveness, surpassing even the performance of lockpicking guns.

It's important to note that each lock requires a specific tool from the Original Lishi product line, meaning you may need to purchase a different tool for each unique lock. However, the KW5 Lishi pick can conveniently be used on KW1 locks, and the SC4 Lishi pick is compatible with SC1 locks. By investing in these two picks, one can gain the capability to successfully open almost any residential door, simplifying the process for locksmiths and lockpickers alike.

While Kwikset and Schlage dominate the market, a vast array of lock types exist. One of the first locks I picked was the Master padlock. These locks, devoid of security pins, offer a beginner-friendly challenge and can be opened relatively quickly. By inserting a tension wrench into the keyway and applying turning pressure while raking the pins, the lock will pop open. Similarly, many residential doors lack security pins, making them susceptible to this technique.

Encounters with security pins become inevitable, and opening such locks may initially seem harder than it is. However, with practice, it becomes an easy skill. The process begins by raking the lock in the traditional manner until the pins enter a false set. A false set occurs when the lock partially turns, mimicking the sensation of being open but halting midway.

At this stage, slowly continue raking the pins until you encounter one that offers greater resistance compared to the others. This is the security pin. By applying upward pressure on this pin while turning the tension wrench in the opposite direction, the tension on the security pin is released, allowing the lock to turn. If the door remains locked, softly rake the pins again until you feel another security pin that exhibits resistance. Caution must be exercised to avoid applying excessive force and potentially bending the pick. Mastering security pins is a significant milestone that separates amateurs

from professional lockpickers.

I use various lockpicking tools, each with its own merits. One particular favorite of mine is the SWICK. It's a remarkable tool I came across through a Kickstarter project. The SWICK's design resembles a folding knife, equipped with 12 unique pick blades. Its compact size and ergonomic handle make it an ideal everyday carry tool for locksmiths and lockpickers. The SWICK offers excellent feedback from the pins, making it very easy to pick security pins. I highly recommend checking it out at `www.picklocks.com`.

If you want to get started with lockpicking, you can find good tutorials on YouTube. However, it's something you have to learn hands-on. I can't wait to attend The HOPE conference to network with other hackers and lockpickers. The conference attracts lockpicking experts and offers lockpicking workshops, demonstrations, and discussions. I hope to see you there.

OOOPS; V97.129

by lg0p89

Cars are an extension of our culture and society. Our persona is reflected in the vehicle we drive. This can be technologically advanced or somewhat basic in the hardware and software included in the model. One commonality seen with the models over the last estimated ten years has been connectivity. In the future, these will be connected to each other, the infrastructure, and other sources. One aspect of this now in use is the owner being connected to the vehicle. Each manufacturer has their own app for this. These can be the Audi MMI Connect, AcuraLink, BMW ConnectedDrive, myBuick, myCadillac, myChevrolet, Genesis Intelligent Assistant, and many others. These are very useful to the vehicle owner now and this is improving with more functionality incorporated into the tool.

With an app, there is a full cycle of testing that generally is done to ensure (to the best of their abilities) the vulnerabilities which are identified through a TARA (Threat Assessment and Remediation Analysis) or other forms and mitigated pre-production. Usually, this process is thorough unless you are there to check the box.

Toyota

Apparently, this process didn't work so well for Toyota. They had a little *issue* that came to light recently. There was a data breach with their online service, the Toyota cloud-based connected service (G-Link, G-Book, and Connected). This service is managed by Toyota Connected Corporation. For over ten plus years, more than 2.15 million vehicles' data was available to unauthorized parties. The timeframe for this was January 2012 to April 2023.

Good News?

The good news, if there is any, is that only vehicles from Japan during that period were affected, not globally which would have caused much more of an issue. There also haven't been any issues noted from the data being compromised, which could have taken the form of the data being misused or leaked to third parties. With the ease of data transportability, this could have been much worse.

Risk

Data is the new oil. The value with this is vast with the data in total, and the many ways you can slice it for the different customers. This includes the vehicle identification number (VIN), vehicle location and time stamp, terminal ID, and video footage. This may sound innocent enough. After all, what are you going to do with a VIN and vehicle location?

An enterprising person might be able to identify individual owners with the data and footage. They could build a file on the individual vehicle usage and location. If you happen to look into the windshield and take a quick picture of the VIN, the database could be searched for the VIN. With this you have the address, and you can search the tax rolls for the owner's name.

Cause

The cause for this was relatively simple. The service was left on for outside access for the cloud instance, or it was set to public access instead of private. This was due to the misconfigured database. It was basic human error. This happens more often than it should. With more companies moving to the cloud in masses, it will continue to happen.

Post-Issue

The corporation set up employee training to increase cybersecurity awareness. They should have turned this off as soon as it was released to the clients. They will also implement a service to also audit the cloud instance setting to ensure this doesn't happen again. While we hope it won't occur again, it probably will... again, and again, and again.

Geo-Distributed Bug Bounty Hunting

by Anthony Russell
@DotNetRussell
https://www.DotNetRussell.com
https://github.com/DotNetRussell

GeoDNS is a technology that allows entities to deliver content to users from servers closest to the requesting user geographically.

GeoDNS is one of the first technologies that a bug bounty hunter may unwittingly encounter when attempting to conduct a bug bounty campaign. Utilizing a geo-distributed cluster of machines enables bug bounty hunters to gain a better understanding of their target attack surface and enables them to map it more accurately. By running simultaneous and duplicate scans from multiple geolocations, attackers can see if a target organization is routing traffic to different servers across the globe based on a requester geolocation. Furthermore, by repeating these scans on a regular basis and diffing the results, attackers can more accurately map a target as new services come online.

Bug bounty campaigns are truly a function of time equals money. The more time you spend looking at a bug bounty campaign, the more you need to earn in order to make the time spent worth it. This means that the more that can be automated and the greater your ability to discover and intelligently parse an attack surface, then the better your chances of finding qualifying bugs while also reducing your time spent. Even with a solid methodology though, there is a major transparent issue that most bug bounty hunters will face at some point, which is a GeoDNS configuration. Attempting to map the attack surface of a GeoDNS configured target without shifting the attacker's location either by proxy, VPN, or some other means, will result in a failure to identify all assets owned by the target organization.

What is GeoDNS?

GeoDNS for the purpose of this article can be summarized as routing a request to the geographically nearest server to the requester that can respond with the requested information. This is not a recent technology and is supported by most major cloud-based platform providers today. For example, Azure Traffic Manager offers a routing service called "Geographic" which does exactly what is stated above. This geographic service (see Figure 1 below) can route a request to different endpoints based on the sources' geographic location.

GeoDNS was developed as a patch for BIND DNS. Developed by Berkeley in the 1980s (Berkeley Internet Name Domain), and originally funded by a DARPA grant. BIND is software designed to interact with the Domain Name System.

It is important to note that geographic DNS handling was never intended to be a security measure. The purpose behind it has been and still is to speed up the experience for the end user, offer redundancy when regions go down, offer a compliance solution for data regulatory requirements, and provide localization of content for end users.

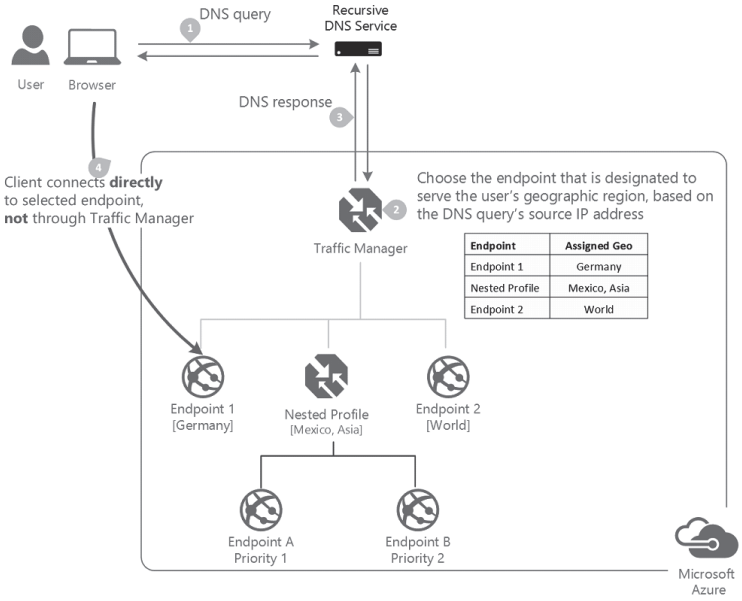


Figure 1

Bypassing GeoDNS

Geographic DNS handling is not terribly complex to bypass. As already stated, it was never meant to be a security mechanism. It is merely something that bug bounty hunters need to contend with.

There are multiple ways to bypass GeoDNS. Attackers can use a proxy server, a VPN, or, as I am going to outline here, a cluster of geo-distributed machines.

Without taking the time to bypass GeoDNS, bug bounty hunters are potentially missing outdated and vulnerable servers that are in scope but outside of the attacker's region. Even if a VPN or proxy is used, it is difficult to iterate between regions to rerun extensive and time-consuming scans repeatedly.

Making the Case for a Geo Cluster Attack Platform

As previously stated, bypassing geographic DNS is trivial, but to do it consistently, quickly, and

automated is an order of magnitude more complex. This is because of the existing options; there is no straightforward way to pivot around the world. It requires VPNs in the geographic region you are targeting as well as the ability to pivot between them consistently. It also requires that you run the same commands against your targets in the same order so that you can juxtapose the regional results. Proxies can also be configured to do this but once again, this requires proxies in the region that you are targeting. If you are using public proxies, they are notoriously unreliable, not to mention the other issues that could go along with running attacks through machines you do not control. This brings me to the heart of this article, which is maintaining a global cluster of machines through which you can proxy commands in an automated and repeatable fashion.

Bug bounties are once again a function of time equals money. Also, since bug bounties are legally authorized by the target entity, the focus can truly be on the target and mapping the attack surface. There is no real requirement to use technology like proxy chains to make it difficult to track attacks back to you. The only primary concern attackers should really have in their bug bounty campaigns is not launching them from a home network and remaining in scope. This is because content delivery network tools like Akamai and Cloudflare will ban the source IP address if they detect malicious payloads being launched against their customers. Getting your home IP address flagged by one of them means you will have a challenging time using the Internet for day-to-day things. This is where the power of using a VPN or proxy server is key.

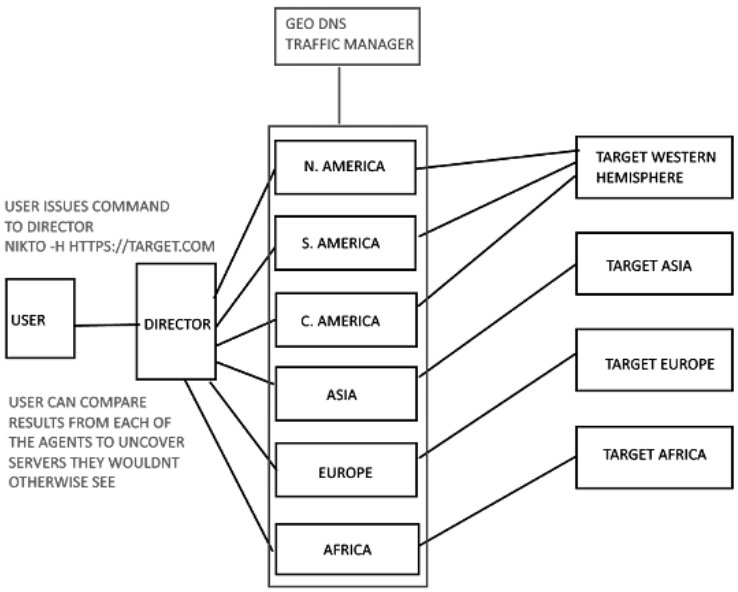


Figure 2

The above diagram shows the proposed cluster setup. The director can be in any region and each of the nodes would exist in a different geographic region. When the attacker issues a command to the cluster director, that command is then issued to each of the regional agents, who then resolves the DNS record and then individually runs the command.

Once this system is in place, some interesting capabilities are then unlocked. For example, the ability to schedule reoccurring recon scans and then automatically diffing the results of the scans to see if the attack surface has changed since last scanned. This is an important thing to consider because targets of the bug bounty campaign do not exist in a vacuum. They are often actively being developed - which means new services, test environments, or development environments may inadvertently become visible to the public Internet. If this happens and you have only run a single recon scan, then you will miss the evolution of the attack surface. This is but one of many additional capabilities we unlock by having a global attack cluster in place.

Development Going Forward

For the better part of 2022 and into 2023, I have been working on a platform that mirrors the above cluster diagram. It is both web and mobile capable. It allows for scheduling repeated scans and attacks, as well as for automatic diffing of results with alerts when things change. This is only a small subset of the features I plan to bring to market with this new tool. For now, most of the feature list is private as well as the repository.

Summary

Bug bounties really boil down to how fast you can find bugs so that you can get paid before the other attackers find them. The best way to do this is by conducting methodical and comprehensive recon against targets. As companies continue to scale, they will ever increasingly use geographic DNS to improve the experience for their customers. The only way to accurately map the attack surface of these companies is by bypassing their geographic DNS systems. Though other mechanisms do exist to do this, it is laborious and often time consuming to do this with existing solutions. This article has demonstrated that by creating a globally distributed cluster of attacking machines, bug bounty hunters can not only get a comprehensive view of a target's attack surface, but also do it in a quick, repeatable, and methodical way.

AWESOME HACKER STUFF AT 2600.STORE

Being a Hacker

by Jo

Since I was young, I've been interested in the idea of being a hacker, the definition of which I'm aware is rather fluid. To be honest, I most likely first heard the term while watching the movie *Hackers*. Even though it lacked any real substance on the matter, it nonetheless was stylistic and pretty damn fun to watch much in the way *Swordfish* was years later. As to why I wanted to be one myself? I'm not really sure, perhaps it was the idea of going somewhere I wasn't supposed to while raising the proverbial middle finger. Maybe it was that by doing so, it meant finding something which had been hidden away, something only certain people were allowed to see, and acquiring that privilege for myself. There was no other real goal involved; it wasn't about changing the world, raising some political point, or financial gain, but rather the pure desire to break through the haze and explore unimpeded. I suppose that's what it means to be a hacker, at least in my view: freedom.

I was born in the late 80s and grew up in the 90s (yes, it really was the best decade Xp) and so was present in an area where the Internet and desktop computers weren't relegated to outsiders and the like, but rather were becoming more and more mainstream.

The first interaction I recall having with such a device was at about the age of seven or so, a period of dial-up, floppy disks, and America Online. I used to play video games on AOL, none of the names of which I can remember, only that one of the games had to do with bugs crawling around and having to use the cursor to squash them on screen. Other than that, I honestly struggled to find much else to do with it. Amazon sold mainly books and not much else, there was no YouTube, Facebook, Twitter, Instagram, and even MySpace wasn't to debut for another eight years or so. That left one to just search and surf through the large amounts of pop-up ads through the relatively simplistic web pages one happened upon.

In doing this, I managed to learn more about what it meant to actually hack something - that there were those out there who knew the languages behind the systems, about study and practice and everything else that a true practitioner of the craft generally needs to know. Then again, I also learned what it meant to be a script kiddie and how passwords could be broken just by entering a bunch of potential passwords in the hope that one would break through. Being one to prefer the path of least resistance, I thus chose the latter.

It started in fits really, nothing overly concerning. Every now and again after scanning through the web in search of information on *Pokemon*, *The Anarchist Cookbook*, and playing on Newgrounds, I'd look for a site, any site really, though I was particularly interested in state or government ones. The idea was to look for an admin page with a login section and type in a bunch of random passwords and keys. Maybe something would happen... that was the notion. What I'd do if it ever worked was another matter entirely. I'm not sure I thought that far ahead, nor about any real consequences.

I failed constantly, as one would expect. Each attempt, after all, was about as brute, simplistic, and, well, stupid, as one such as myself could manage but somehow after doing this on and off for a good long while, at some point it actually worked. Even now, nearly two decades later, I can remember the site page changing as it accepted whatever gibberish I had entered and I was in. As to what the site itself was, I can't fully recall that part either. I had tried so many, the most I can make of the success was that it was on a civilian site I had most likely mistaken for something either state or federal. I also recall it having to do with retired police officers, a list of which was then opened to me, along with their information. In hindsight, the most likely culprit was something akin to the Association of Retired Police website. That said, it was still an unexpected result.

When one breaks into a site, there's the initial high, that feeling of "Damn, I did it, wait, how? It worked, it worked!" Everyone probably has their own unique reaction, but mine at the age of ten or so was to freeze, realize that I had done something that could get one into a good deal of trouble, and log out

soon after without saving anything, whether it be the data from the site or a copy of the credentials used to get in in the first place.

From there on, I slacked off on any similar attempts. Having accomplished something I'd initially intended on doing, this somehow made me feel at least somewhat satisfied. I suppose it's worth noting that at one point down the line, I became a bit enamored with viruses, but due to my still considerable lack of programming knowledge had very little idea of how I could further examine or make use of them. Honestly, I think it was just the idea of having something seemingly cool and destructive at my command that made the subject as enticing as it was.

This lull in both interest and study on the subject lasted, well, until I was in my thirties, much closer to the present. Frankly, it's hard to believe that I'm now 35, but I'm a staunch believer that one can remain as young as they feel until the moment they keel over dead. With that being the case, I still count myself as a particularly angsty 14-year-old (I'm not even sure if I'm being serious or cynical right now).

The rekindling of both my desire and willingness to learn more in the field of computers, programming, and what it means to truly hack came about after a decision to pursue cyber security as a career choice.

They say one's never too old to return to college, something that unbeknownst to me was somehow taken to heart. For the past 15 years or so, I'd been a third-shift security guard and had lately decided it was probably a good idea to start considering something a bit *more*. That said, already having an associate's degree in criminal justice, it made the choice to go for a bachelor's in cyber security all the more logical. It was pretty much a leap from protecting people and property physically to doing so virtually.

Of course, my intentions weren't entirely financial, nor benevolent. I was merely following a path I thought would be doable. In addition to that, it was guessed that skills taught in a college-level program could not only teach what was needed to move up in the way of a better job but also allow me to pursue my more curious if not dubious hobbies that had until then lay dormant.

The course provided was to be two years with an unpleasant assortment of statistics, calculus, form and essay writing, humanities, several programming languages, and finally after all of that was out of the way, the actual classes dealing with cyber security itself.

As of this writing, I'm about six months away from graduation, having finished the majority of it all. I understand that the math portion is to teach critical thought and how to pursue a task logically, but I nonetheless hated/hate it with a passion. The programming, less so.

Programming is like any language - it requires practice and passion to not only learn but keep ingrained over the long term. The people who become truly wonderful programmers are the sort who not only learn it from others, but continue to practice and hone that ability whenever they can on their own.

Suffice it to say, I didn't have that passion before and still don't. Of course, I knew this beforehand. It's why I chose cyber security over, say, computer science or software development, primarily because at its core it dealt more with using already present tools and systems rather than having to create the same from scratch. Again, it was the notion that it was doable and, after having taken these first steps, has been undoubtedly worthwhile. After all, it's because of it that I've been able to fully appreciate the Linux operating system and the beauty of virtual machines, explore the dark web, converse with interesting people in shady chatrooms that look strangely similar to one Neo was in at the beginning of the first *Matrix* movie, peruse the long lists of illegal substances and products shown on Silk Road-esque storefronts, and have wonderful fun with penetration testing software.

In the end, knowing what I know now has shown me how talented some people are, just how much effort goes into learning these skills, and what can be done with them whether they be white hat, grey, black, or otherwise. There's a difference between seeing something and doing something, obvious as that sounds. It gives you a much more significant appreciation for it all and shows you just how much further there is to go, staying with you in the back of your mind and nudging you forward all the while.

Byte-Sized Justice: A Tale of Hacker Ethics and Copy Protection

by The Mage

In the Summer 2023 issue of *2600*, Albert Einstable shared an intriguing anecdote about a method to disable a program if a customer ceased subscription payments during the early days of personal computing. Inspired by this, I've decided to recount my own related, albeit much more mischievous, tale about my unique way of dealing with the unauthorized use and theft of my code.

Rewind to the early 1990s, a golden era for hackers and telecommunications. I was on the brink of my teenage years but already seasoned in programming, hacking, and online communications. Living in a somewhat isolated rural area - about a two to three hour drive from any major city - left few opportunities for rubbing shoulders with fellow coders or hackers.

My lifeline to the hacker community from this remote location was the world of bulletin board systems (BBSes), a thriving hub of communication for technology enthusiasts like myself before the concept of the Internet and online services took shape in the mainstream. I had been accessing various BBSes for a few years and even created my own when I was 10. By 13, I was sharing source code for my security tools and applications on my BBS, seeking feedback, and eagerly entertaining suggestions for features and improvements.

Considering my age and the era, licensing and copyright topics didn't cross my mind. My joy was in coding, shaping my programs based on other people's suggestions, and connecting with other hackers. I had many users dialing in daily to partake in the online games I designed and hosted, to download the security tools I created, and to communicate using the forums and messaging system. However, the peace and tranquility of my BBS were disrupted when a semi-local BBS, located about an hour's drive away in a different area code, started plagiarizing my code, modifying authorship details, and reselling the compiled applications as their own.

This was an era when people generally accessed a BBS only if it was a free local call. Thus, they most likely assumed that their theft and unauthorized distribution of my content would fly under the radar. However, I had my ways of avoiding call charges and therefore kept a vigilant eye on many other systems, including this dishonest one.

As a 13-year-old, utterly engrossed in hacking computers, playing video games, and listening to alternative rock music, the idea of someone profiting from my creations was downright irritating! Even more so when they were reselling my security/hacking utilities and business tools, indicating a significant lack of technical competence or sheer laziness to do anything beyond modifying a few text strings and recompiling the software so that they could profit.

At one point, in response to a user's request, I shared the configuration files of my BBS to help them establish their own. This enemy BBS operator had no qualms about using those to replicate my system, down to its look and feel. And, in an amusing display of oversight, he even forgot to change the BBS name! Although a friend found it funny when he stumbled upon the obvious replica, I was not amused.

Being relatively introverted and young at the time, directly confronting someone I assumed was an adult who may escalate things into physical confrontation was not an option that I was willing to pursue. I was not about to stop coding or sharing my work either. This was a vital creative outlet, a gateway to connecting with other hackers, and a launchpad for many exhilarating cyber-adventures.

I decided to address the issue my own way. At that time, I was working on a security utility that I knew would be a tempting high-value target for this deceitful BBS operator. Given my assessment of their technical skills and overall intelligence, I slightly altered my usual approach for this utility's release. Instead of providing the complete, uncompiled source code, I pre-compiled a library file essential for compiling and executing the utility, including clear instructions on how to do so, in anticipation of their technical ineptitude.

Within the source code, I explicitly mentioned that the code was shared for educational purposes and to garner feedback. I welcomed modifications and was keen on seeing people's creative extensions. However, I emphasized the prohibition of changing the name of the application or author.

Additionally, I include a disclaimer stating that I, the author, offered no guarantees about the code's execution, error-free operation, or the absence of unintended consequences if modified. In retrospect, I suppose I assumed this was a common understanding, but I felt compelled to state it explicitly now.

My "copy protection" was nestled in that pre-compiled library. In its simplicity and perhaps dramatic flair, it was designed with a singular target in mind: the persistent thief. On execution, the application checked the value of

the variables containing my name. If modified, the copy protection would spring into action.

I could have designed it to simply halt the utility or display an error message indicating a modification. But I had a more drastic plan. My protection corrupted the File Allocation Table (FAT), causing the computer to lose track of file locations. Furthermore, it deleted the Master Boot Record (MBR), effectively immobilizing the computer as it would lose its bearings and be unable to locate the operating system upon being powered up. If this enemy to my state wanted to play rough, I was in.

When I was ready, I posted the utility. I set a login alert for their account, so I was notified and able to watch as the hostile BBS operator logged in and downloaded the utility's source code, leaving me to wait in anxious anticipation.

This was a time when antivirus (AV) software wasn't widely prevalent, but that still left room for uncertainty about whether my code would execute. Moreover, I hadn't tested it myself. I was young and poor and didn't have a system I was willing to brick to ensure its effectiveness. And then there was the off-chance that the operator had system backups to recover from a decimated MBR and lost files. All of these potential modes of failure were running through my mind as I saw them siphon the bits and bytes of my latest utility over the phone line.

Then another concern struck me: What if an innocent coder downloaded this, merely seeking to learn from my work? Swiftly, I pulled the code offline, disabled the destructive functions, and re-posted it, ensuring no collateral damage.

A day later, I called the thief's BBS using an untraceable account and phone number. There were no signs of anything amiss, so I logged off. Then, the next day: *Ring*. *Ring*. *Ring*. No answer.

The following days also yielded only unanswered calls. Finally, a message on another local popular BBS revealed the indefinite offline status of the thief's BBS due to "irrecoverable computer issues." While I couldn't definitively attribute this to my "copy protection," the satisfaction was undeniable, and I indeed achieved the ultimate result, as he never tried to steal my code again.

While I wouldn't advocate such drastic measures today, my younger self felt justified by the explicit warnings, labels, and disclaimers I had included in the code. Nowadays, advanced and readily available tools offer far safer and more effective ways of code protection, though perhaps lacking the thrilling edge of my youthful ventures.

As I conclude this article, I'm reminded of the wise lyrics from Exode, the legendary 90s punk rock hacker band, from their track "Basement Laboratory."

All above is solemn truth,
Heed this warning intrigued youth,
Those who don't believe my tale,
You're rodents anyway.

A Quick Intro to Biohacking

by microbyt3

In the vast realm of hacking and technology lies a magnificent field: that of biohacking. While the term may conjure up images of techno-thrillers and *Snow Crash*, I assure you it is a real field that encompasses an intersection of biology, technology, and most importantly, hacking! Biohacking is, to make it short and concise, applying the hacker ethos to biology and sidestepping the normal way of doing biology in the process. In this article, we'll delve into the world of biohacking.

DIYBio

One of the most fascinating and important aspects of biohacking is its thriving community of DIY labs where, instead of having large universities or for-profit companies as the driving factor of progress, biohacking tends to be driven by small, community-led, indie labs, democratizing access to biological research, so that the normal person can try getting their hands dirty. These DIY labs have expanded all around the world, from New York City to San Francisco to Brussels to Budapest to Paris to Bangkok to Singapore to Tokyo - you get the idea! Before these community-led labs, biology research was only open to a small cluster of professionals and now, thanks to biohacking, it's open to everyone!

Just like hacking, the ethos of openness and knowledge sharing is central to biohacking. Biohackers, like normal hackers, are driven by curiosity and passion for biohacking, and as such believe in the democratization of scientific tools needed for this, primarily through the aforementioned indie labs. In line with this philosophy, many biohacking labs offer workshops and programs. These initiatives provide opportunities for people from diverse backgrounds who may not be able to really do any biology work on their own (e.g. someone may be priced out of academia or need to look after aging family members)... really anyone who wants to learn about the latest advancements in biology, acquire hands-on skills, and collaborate on innovative biohacking projects.

CRISPR/Gene-Editing

When someone thinks of the term "biohacking," one of the first things that tends to come to mind is gene editing. Gene editing is a stunning, fairly recent invention, with CRISPR ("clustered regularly interspaced short palindromic repeats") the main driving force behind gene editing, having its discovery kickstarted from 1993 to 2005, and its gene

editing usage being discovered, or more accurately, invented, by Cong et al.[1] at Broad Institute of MIT and Harvard.

CRISPR works, in short, essentially by cutting out a gene and modifying its repair mechanism in a truly fascinating process which I don't have space to explain here. CRISPR has two possible results, both of which are beneficial when trying to study a gene. The first possible outcome is the gene is "knocked out," which means that there is an error in the DNA, not necessarily the As or Ts or anything mixed up, but rather a physical problem and, in this case, the cell cannot use the DNA. It is as if part of a disk is corrupted. These knock out genes are useful for scientists, as seeing what happens without something is very important for reverse engineering a cell. The other possible outcome is replacement of a portion of the DNA with another part of DNA. This is significant for the fairly obvious reason of being able to make the cell do something it wouldn't normally do. This also has some highly important aspects, such as being able to prevent hereditary gene-based diseases (like Werner syndrome).

Grinders

These people - grinders - captivate me through what they do. A grinder is a biohacker who uses body implants to become a literal cyborg, to transcend the limits of a normal mere mortal. The functioning of grinders, as in the ability for the human body to be OK with what they do, I find wild. An example of what they do is implant RFID chips inside of their bodies, like in their hands[2]. Imagine breaking into a building with a cloned RFID chip in your hand, or how easy cloning an RFID card would be if your hand would just "slip" without anything special in it.

Another aspect of grinders is neural implants. While few of these actually exist, the main closest relatives are prosthetic limbs which use electrical signals from neurons to determine how to move themselves. However, recently, we are seeing a massive uptick in the capabilities of neural implants - such as Neuralink - whose brain chips are expected to have clinical trials soon[3] (however, a lot of the monkey subjects did die, but I personally do trust the FDA, so while I'm *not* going to use one, I think it may not be as bad as it sounds).

Biosecurity

Because of all this growth in biohacking, especially because of grinders, biosecurity is starting to become an important topic. Biosecurity is, as the name describes, cybersecurity but for biological devices. This has been popular and at least commonly heard about for a while now with notable hacker Barnaby Jack doing presentations on some of the more important parts of biosecurity, such as pacemakers and insulin pumps. Biosecurity is becoming even more important in recent times, however, due to smart technology starting to make its way into medical devices, along with the previously mentioned newly formed brain chips. Biosecurity is really going to start getting important. We don't want brain ransomware, do we?

Another section of biosecurity which gets more attention than the previously mentioned parts even though it doesn't deserve it is engineered pandemics. While engineered pandemics are a problem, most of the suggestions people have on how to prevent engineered pandemics tend to be about regulating - primarily intranationally (i.e., preventing citizens from doing it). This solution to engineered pandemics is not going to work for the same reason that engineered pandemics are over-hyped, which is that engineering a virus or bacteria is extremely difficult. You have all the challenges with culturing viruses, but then adding genetic engineering for increased infectiousness makes it something that an indie biohacker - which is mainly what this article has been about - can't feasibly do.

Resources

The following are some resources to learn more about - and get involved in - biohacking:

- *DIYBio* - `diybio.org/local`
- *OpenWetWare* - `openwetware.org/➥wiki/Courses`

If you find your local biohacking lab on the DIYBio local lab section, you should check if they do courses or programs. If they don't, remember that you can always ask through an email or DM, and most likely the person on the other end would be more than glad to help a fledgling biohacker find their wings.

For learning about biology in general, I suggest:

- *MIT OCW* - `ocw.mit.edu/`
  They have a lot of courses on biology.
- *Libretexts* - `libretexts.org/`
  They have books on biology, medicine, and chemistry (which is usable for cell hacking).

Conclusion

Briefly, biohackers are essentially people who apply the hacker ethos to biology in order to try to - like hackers - create a better world. They use indie labs, fascinating science, and body modifications as some, but not all, of the means to their end of a better world. They also run numerous small, community-led labs, which I encourage you to get involved in.

Thanks for reading, and don't stop hacking!

[1] `pubmed.ncbi.nlm.nih.gov/23287718/`
[2] `dangerousthings.com/product/next/`
[3] `www.reuters.com/science/elon-musks-➥neuralink-gets-us-fda-approval-➥human-clinical-study-brain-➥implants-2023-05-25/`

The Hacker Perspective

by Derneval Cunha

The first thing that enters my mind when an unknown guy introduces himself as a hacker is "he must be nuts." The second thought is "even crazy people might have some good information." The third thought is "it might be a setup." Because most of the time, there are no hackers in front of me. There are people trying to save money, people who want to unblock their smartphones, people who want to find out about their girlfriends. And people who want to sneak into places they don't belong.

I might as well tell my story. I started as a nerd and didn't play soccer (which in Brazil was pretty rare). In 1982, I went to Europe. In London, there was this *Tron* movie in the theaters, and the Osborne computer was available for sale - a dream for a sci-fi fan like me, but out of reach. In France, I did some phreaking (check the YouTube "Gardel's Ghost" video). Once I almost got arrested. In all, I traveled and lived in an "alternative lifestyle" for about nine months.

Back in Brazil, I visited a relative of mine in Brasilia (Brazil's capital) and he introduced me to the "computer scene" there. Or, should I say, "kids addicted to Spectrum computers and the video games scene." He taught me a lot about that strange new world, all centered around computer shops, BASIC language programs, and video game arcades. As close to the *Wargames* movie as it could be in those days.

Long story cut short, years later I passed the entrance exam for German literature at the University of Sao Paulo. No tuition fees and free student housing. It was not computer science, but resources there were not scarce. There were lots of computer labs throughout the campus, mostly PCs with 512k memory. (In those days, that hardware was worth about US $2000.) There were even computer labs open 24/7 like in the Polytechnic School of Engineering. I went there and it took me about ten minutes to team up with the "computer gang." We were all "computer pirates." They called themselves "rataiada" (bunch of rats).

Time passed and I achieved the dream of an internship - just to research the Internet. My job was to keep doing telnet, ftp, etc. for 20 hours a week for those days in 1993 and 1994 when there was no Google.

In October 1994, there was a "hacker and virus conference" in Buenos Aires, Argentina and that was another life changer. Argentina had a strong computer virus and hacking scene, but most people were BBS-oriented. The study of computer viruses was a really popular theme everywhere in the world at the time. There were about five virus ezines and a paper publication, *Virus Report,* that organized the whole thing.

My Internet research (at my internship) was about computers and education. But I also got to be a guest speaker. As such, I gave interviews and did some networking with an MIT virus researcher who gave me a CD packed with lots and lots of docs, info it would have taken months and months to find and even download in those days. I also learned how to write articles in magazines.

Back in Brazil, I started to be known as a "hacker." Great powers and great responsibilities. The hacker ethic was still new for me, but I had gotten so much knowledge... it seemed a shame not to share. It got into my head that I could be the first Brazilian guy to write and publish something on the subject and inform people about that hacker universe. I first tried the paper press. But no journalist was interested in computers and hackers, something which changed after *The Net*. (By the way, TV people interviewed me about that movie and a review from *2600* helped me.)

So to spread the word about hackers, I started a "hackers" list and a magazine for fans - known as a "fanzine." I called this electronic fanzine an "ezine." Paper fanzines were nothing new, but my idea was a jackpot. Both the (not Usenet) list and the *Barata Eletrica* ezine were a hit. They went viral. Journalists started to look for me for interviews and to help with articles (many times an "interview" turned out to be nothing more than a quest for help with an article). The Mitnick arrest made headlines and created more of this.

Being a one man show, it was tough. I had to write most of the articles. I had to think them. I had to edit the zine. And I had to distribute it on the Internet. People wanted more articles

teaching "dark subjects," but the Internet there in Brazil was still such a baby. I even used my real name. My signature had my name, a paper mail address, and the phrase "I login, therefore I am." (My efforts paid off - a few years ago, a top brass from the cybernetic section of the Brazilian army introduced himself and shook my hand at a security conference in Sao Paulo.)

In 1995, I went to London again, this time for the Access All Areas conference. It wasn't the same as HOPE or HEU, but I ended up being the first guy to write in Portuguese about a lot of subjects like Echelon (check the documentary *Echelon: The Secret Power* on YouTube). I met friends from Argentina, later went to Amsterdam, and hitchhiked to Berlin to visit the Chaos Computer Club.

Back in Brazil, I helped start a once-a-month hacker meeting in bars and restaurants. Sometimes there were huge gatherings. I would always talk of the wonders of Linux.

I basically hacked together a hacker scene in my country: hacker ethics, government surveillance, digital citizenship, hacker meetings, electronic publications, you name it. My *Barata Eletrica* ("electric cockroach") ezine was read everywhere, on BBSes and the Internet. First it spread by email, then Usenet, then the EFF hacker library. When the first Brazilian websites started to appear, there would be links to mine. And I paid attention to tags. For a time, my ezine would always come first in Google searches.

That was the "honeymoon." By 1996 and onwards, it was like a "marriage." With the commercial Internet, more people started logging in and some of them confused nuking, defacing websites, taking control of computers, and phishing scams with hacking. Out of fear, I did not write a book. I didn't want to be confused with "copycats." To top it off, I was jobless. I suspect I was "blacklisted" too, as people would not hire me.

The tide had changed and I can't say I didn't see it coming. And then I felt some stabs in the back. Magazines were publishing articles pretty close to "how to be a hacker." And people were publishing fake "how to be a hacker" books using my material. I could have sued people. But suing might have given them more publicity. And I could have lost. It's not easy to explain, but thinking about it, if you are famous, things can get a bit out of control.

There is a popular quote here that says "pork snout is not an electrical outlet," but after years of explaining to people what hacking is all about, I am proud of myself. I never had to hire any lawyers and explain things to a judge in court in order to avoid jail. What I did do was change my style, and tell everybody the dangers of writing zines. That took some time, but stopped the flow of copycats.

By the turn of the century, there was so much bad press about online vandalism that people who attended those early hacker meetings asked to be forgotten. There were "hacker conferences," but for me they were just a chance to meet foreign guests. The IT job market is really tough when you're over 40 even if you've got the right certifications. No job offers except maybe selling IT security products.

A few years ago, I went back to the university. I thought maybe learning math would enhance my chances of working with computers again. There was this opening for an internship dealing with Linux administration in the students' computer network for 20 hours a week - the sort of thing one does as a hobby. I even got as far as training for the job. Then they changed their minds and did not hire me. But I didn't care. I knew I would be back at the top. There will be a day for people like me. We are survivors.

Let's be smart enough to see beyond our capacity. We can't even be sure democracy will survive. It's a whole new world. In Sao Paulo, working at home proved to be such a hit that whole office buildings are now empty for good. Perhaps "hot" office locations like Paulista Avenue in Sao Paulo, Manhattan Island in New York, or The City (London) all will be replaced by people working in suburbs or apartments. And people might never move from their home towns to live in big towns in search of education or better jobs. Maybe it's better for people in the IT industry. Soon people will invest more and more cash into hardware.

One trend which is quite appealing in my opinion is fixing things instead of buying, as well as developing low-cost wares that replicate apps or hardware that people have to pay exorbitant prices to own. Looking back in the history of the computer industry, IBM only started to develop low-cost PC machines because people were already crafting and selling low-cost computers. Now, with hundreds of thousands of people who are working, studying, and living lives inside their houses (if they are lucky enough to have a roof over their heads), they need to have cheap alternatives to hardware that will allow for that long distance interaction.

My advice to future hackers? I prefer "common sense."

Never ever claim you're a hacker or anything like that. If you're good, people will notice that. Suppose you want to impress family

and friends and adopt such a life. People will probably ask you to teach programming, check their computers, or upgrade their software, hardware, etc. And because "information must be free," they won't talk about money. Of course, if something goes wrong, it's on you. The computer was OK - you destroyed it.

Even when it was mostly on BBSes, people with very little computer curiosity or experience wanted to copy things they saw in the movies. They bought a computer, a few books, and "tried to hack NASA." Don't do it. If you do get famous, chances are you won't get a big paycheck out of it.

When dealing with and researching "gray area stuff" (like Bitcoin), it's a good idea to encrypt all important data, have a copy of that stuff somewhere safe, and have someone you trust who can go to your place to water the plants, pay the bills, etc., in case you can't. It's best to be prepared.

It seems likely that sooner or later in life, everybody is gonna go to the police for one reason or another. It always helps to know something about how they work and to have the name of a good lawyer in your pocket. An old police investigator gave me this advice: never ever have a selfie with police or pictures of weapons on your smartphone.

Maybe somebody wants you to check someone's computer because that will help with some sort of investigation. Well, with great powers come great responsibilities. Methinks curiosity killed the cat. Think ahead because there are times you "lend a hand" and later on you "just want your life back." It happened to me.

If you want to be known as a hacker and dream about IT security jobs, my advice is to submit articles relating your findings to publications like *Phrack, 2600*, etc. It worked for me and changed my life. And you can brag to nice girls and friends that you're a writer.

Next, use that blue box t-shirt once in a while. It works wonders for networking, like when I was in a famous "underground" nightclub and was spotted by the author of the Brazilian phreaking manual. In that near darkness he recognized the t-shirt.

It is funny, but one can make enemies even by minding his/her own business. Soon or later in life, you'll find out how people you trust are stabbing you in the back. You have to have a Plan B. You're going to have to deal with that.

Never think you're a smart guy. Sometimes it's just beginner's luck.

HACKER PERSPECTIVE SUBMISSIONS ARE STILL OPEN!

Don't expect this to last for much longer, but we're currently accepting pieces 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 (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.)

Privacy: Protecting Your Personal Information Online

manish.mradul@gmail.com
by Manish Mradul
www.linkedin.com/in/manish-mradul

With the growth of technology, the ways of marketing have observed a paradigm shift. In the past, the marketing agencies and corporate sector used banner display newspapers, magazines, or television and radio broadcasts for the publicity of new products to a larger audience. In today's world of artificial intelligence, the marketing agencies are using "The Internet" to meet their publicity goals. Through social media, individuals generate vast amounts of personal data online. This data is collected and sold as big data to the corporate sector to be used in data warehouses. Data warehouses are used to analyze big data to generate visualized results that may be used for decision making such as analyzing trends, predicting the potential of a new product, understanding the targeted audience, and generating new sales and marketing plans. Advanced big data systems can access and analyze this information easily, creating a big privacy concern. Although many corporate firms use this data to generate personalized results to meet user demand, there still exists the vulnerability that this confidential data might be misused. In this article, we will discuss how you can protect your confidential data, improve your privacy, and surf safely on the Internet.

What Are Big Data Systems?

Big data systems are systems that store and analyze a huge volume of data to generate personalized results. It uses multiple techniques such as data warehousing, data mining, machine learning, visualization, etc. The data can be gathered from various online activities performed by users as they surf through the Internet every day. Sources from which the data is collected are heterogeneous in nature. This data is passed through an extract, transform and load (ETL) phase before it is used for analysis. This process takes place in a data warehouse. Big data systems use machine learning algorithms to divide different categories of audience or product types into clusters or predefined classes. Once the model is trained, data of a new person is then compared with the existing clusters or classes and the person is then added to a particular group of people defining the targeted audience for different companies. Hundreds of clusters are generated from big data to create a baseline for user activity in order to predict what the user is interested in, what the current need of the user might be, what the user might need in the future. Based on this baseline, important decisions are made such as changes in existing products, launching new products, generating advertisement based on current trends, etc. Another famous technique used by big data systems is web mining. This technique enables the systems to take data from the search history of a person or what the person scrolls through on the world wide web. Based on this data, personalized website content is generated such as the Facebook feed. Many important events in the past have been successful due to the decisions made by analyzing big data.

Why Is This a Problem?

While big data is a useful tool for organizations and decision makers, it comes with users' privacy being compromised. Social media or web users share all kinds of data online that can sometimes be highly confidential. While it is a threat for users, it is also a negative point for the corporations as users lose trust in the websites that are not secure, leading to a loss in traffic. This may lead to low sales through e-commerce websites. With all the information available to the corporate sector via big data systems, the minds of people can be manipulated to alter their interests, political views, and lifestyle in a way which benefits the organization. Additionally, these analyses can reveal sensitive data of the users, which may cause damage if it is misused, such as transaction records, location, travel history, etc.

What Can a User Do to Protect Personal Information Online?

Data confidentiality, integrity and availability are three essentials of data security. Here are a set of steps that you can perform to make sure your data is secure:

Come up with a good and unique password: Passwords are used to shield and differentiate an individual's data from the general Internet public. Make sure that you use strong and unique passwords. Strong passwords are the ones that meet complexity requirements. Such passwords are difficult to guess or even memorize if someone takes a quick glance while it is being entered. Sometimes even after using a strong password, your password gets leaked or your account gets hacked by a person using other means of entering your account such malicious software or phishing links. To protect yourself from that, it is important for you to ensure that these passwords are changed frequently.

Enable two-factor authentication for your accounts: Two-factor authentication (2FA) is a dual layer security technique that requires you

to provide two forms of passwords to log into your accounts. This includes a password and a code sent to your phone or email. Two-factor authentication can help prevent unauthorized users from getting access to your accounts even if they have gotten your password by some means. The second code is unique every time and is sent to a phone number or email address that you provide. Most popular social media platforms such as Instagram and Facebook offer two-factor authentication to ensure data security and safety from hackers.

Be mindful what you share on the Internet: One should realize that the data shared on the Internet is at risk of being leaked by attackers. Therefore, it is important to avoid posting any kind of sensitive data that may cause harm if it is leaked. Confidential data may include your financial details, your identification details, travel history, etc.

Enable desired privacy settings: Privacy settings include a variety of controls that, for example, define who sees your data online, who shares your data on their accounts or social circle, who sends you messages and requests, who sees your activity status, how many devices log in to your account, as well as blocking and unblocking accounts, etc. Apart from social applications, most browsers also allow you to enable your desired privacy settings for yourself or for your children using parental controls. These can be defined from within the browser's settings. Good privacy settings enable you to decide where your data goes.

Enable virtual private network (VPN) extension: Virtual private networks or VPNs are commonly used networks that are provided by proxy servers or VPN applications to allow users to surf through the Internet with a masked IP address. Think of VPN as a tunnel. A vehicle passing through the tunnel cannot be observed by the people outside that tunnel. Just like that, a VPN provides you a unique link to surf the Internet with additional privacy by masking your IP address and location, as well as additional features like malware protection and ad-blocking. Many VPN apps and browser extensions are available on the Internet with free and paid versions.

Do not click on suspicious links: A common trick used by attackers is to share infected links that are used to download malware into your computer. This malware is used to obtain unauthorized access to your computer to get your personal data - which might be highly confidential. Scammers create phishing links to rob people by tricking them into sharing their bank details. To protect yourself from this, it is important that you only open links that come from authentic sources.

Do not download software from unauthorized websites: When you download cracked versions of paid software using illegal means, you often have to face the consequences of viruses being downloaded into your computer. Many people use torrent files to download software and media (movies or songs) from other peers. An attacker can easily connect to these networks and share malware. It is important that you download software from authentic sources and publishers.

Check digital certificate before accessing any website: Websites that provide a secure experience are always certified by a trusted third party. These third parties provide a uniquely generated digital certificate that ensures that the website is authentic, secure, and verified. To check a digital certificate, click on the lock symbol on the address bar. Click on "Connection is secure." After this, click on "Certificate is valid."

Make sure that your confidential data is encrypted by the platform: Encrypted data refers to the data or message that is converted from plain text into cypher text which is only readable to the person having the correct key for it. Encryption ensures that the message is only read by the authorized party, keeping in consideration the high confidentiality of the message. Many social applications such as WhatsApp, Telegram, Viber, and Facebook Messenger.

Use anti-virus software: Anti-virus software is a tool used to cope with the problem of viruses. Make sure to use anti-virus software to scan any attachments or downloads before opening them. This can help detect and prevent malware from infecting your device. Anti-virus software protects against viruses and malware, scans email attachments, helps prevent identity theft, and provides real-time protection.

Conclusion

With the increase in technology and the use of the Internet, marketing methods have faced a paradigm shift. Big data systems are being used to make important decisions in the political and corporate sector. This change has its pros and cons. These days, people share a lot of personal data online that may include their personal opinions, interests, and identification details. It generates a concern for users' data privacy. By following the steps suggested in this article, one can ensure safe search and usage of the Internet.

NEW HACKER SHIRTS AT 2600.STORE

The AI Risk Nobody Seems to Mention

by Felix Atter

It's coming for our jobs!!
It's going to start Skynet!!
It's a threat to our privacy!!

We have all heard the big scary talk about artificial intelligence (AI). I opened with the three I hear most often and each of these can be partially or completely eliminated as a risk if managed properly. I can dive into them, but many other articles from many other organizations have done so extensively.

I want to talk about the fourth horseman of the AI apocalypse. This is not about sowing more fear, uncertainty, and doubt in a world saturated by it. This is about taking sane steps to ensure neither you nor the company you might work for gets tripped up again by a well known trope. We cannot trade away our next generation of experts without paying for it. Let me explain.

I remember when everyone I knew in a tech job got started as a low level help desk operator. They would then vary and either work through college or move up through the ranks. When we as an industry moved those help desk jobs overseas, it was a fantastic boost to profitability, and in some cases even the effectiveness of the help desk.

This is not some xenophobic rant. It was a great process when done right. The issues really started about five years after the bulk of large organizations started to do this. Suddenly, finding a senior help desk admin looking to become a junior systems administrator was not so easy. A couple of years later, even finding cost-effective mid-level system admins was a fight. We sold off the farm team. Entering the IT work force no longer had a well known gently sloped on ramp. You now had to jump into either a help desk manager role or do enough schooling to actually jump straight in as a network engineer or server admin. It took us years to recognize the issue and correct for it.

Now consider AI. I have spent the past several months learning more and more about it and talking with people across several industries, and there is a mix of curiosity, fear, and even open doubt regarding its future. I see article after article talking about how it will replace creative jobs, how general AI is right around the corner (it might be), and how it is a huge gaping hole in our data security if used wrong, as Samsung found out in May 2023 when they restricted generative AI use after an employee uploaded sensitive code to ChatGPT.

From all that conversation and research, the one risk I am most worried about is the idea that it will take the place of the humble paid intern. If we look at what large language models (LLMs) like ChatGPT are really good at; we find they are fantastic research assistants to mid and senior level technical assets from governance risk and compliance (GRC) folks to developers and DevOps engineers.

Last time we eliminated a wide array of entry level work chasing efficiency and profit, it took most of a generation to recover and adapt. This shift from hiring entry personnel to do leg work to letting a bot do it faster and more thoroughly sounds like an amazing opportunity. To be fair, it's exactly that. It's just not a free ride. It's like we climbed the rope and now we are pulling it up after us. Those who come after will be forced to climb even higher up the IT/InfoSec tree before they can try for a job.

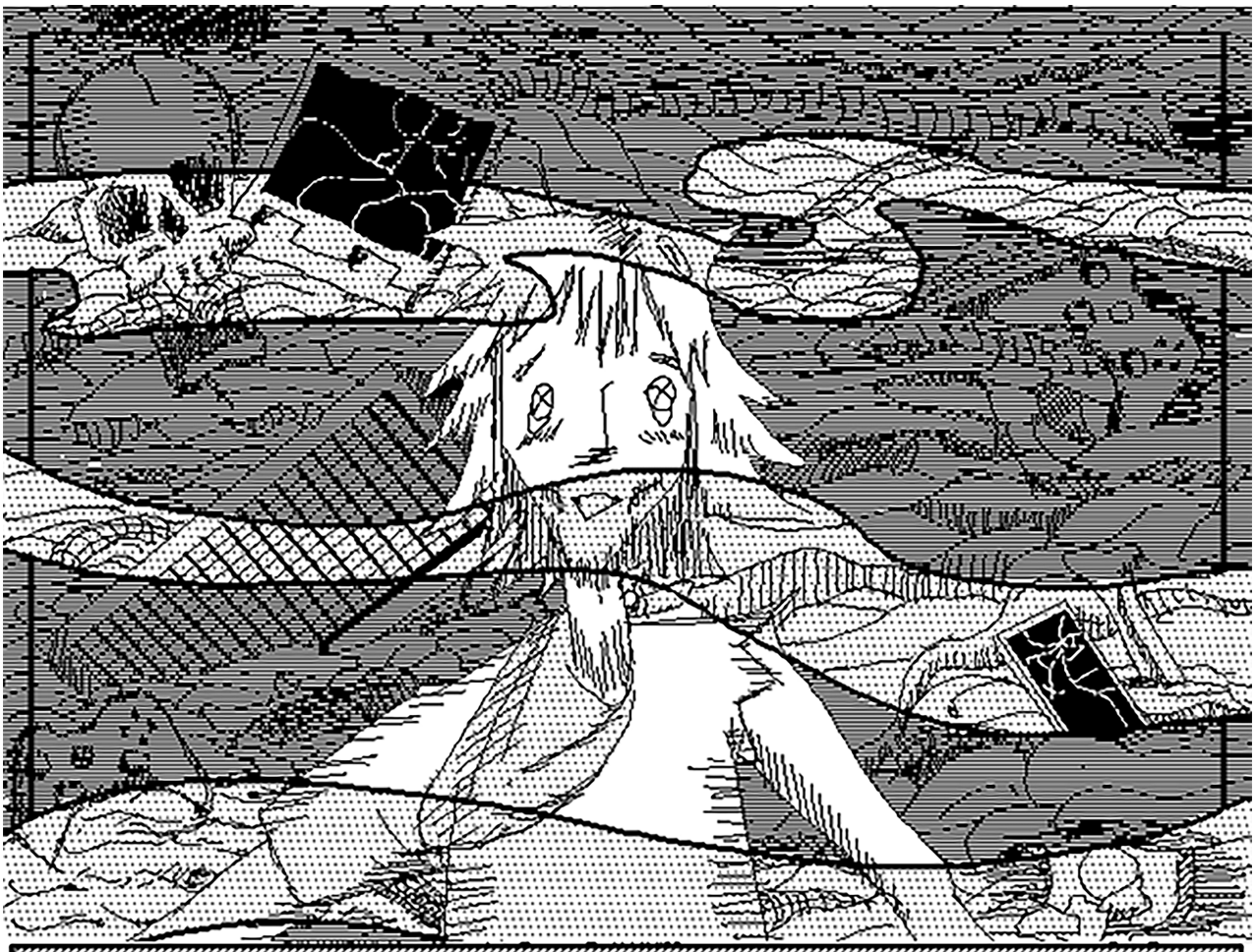
So what do we do? Hold still and hope it goes away? Rage on forums and article comments about how it's all terrible? Pass laws trying to restrict access?

We know those will happen. We know those are unlikely to stop the forward march of progress. My simple advice is this: Advocate within your teams and friend groups that current generative AI is not a replacement for human insight.

We are at a crossroads where teams all over the world are seeing an opportunity to accelerate their projects and reduce costs. My one glimmer of hope is that this will be just as valuable to students, young engineers, and hackers in our community. I learned much of what I know from classes and books. These days I learn 80 percent of the new things I know from videos or even shorts. Tomorrow maybe it will be AI I use to design a lab just to see if I can fix what they got wrong.

This has been called the next revolution, just as the Industrial Revolution and the information revolution changed what it meant to create or to work hard. I don't believe we can stop it or put the smoke back in the circuit board. I do believe it is up to us to leave a path open to those who will follow us.

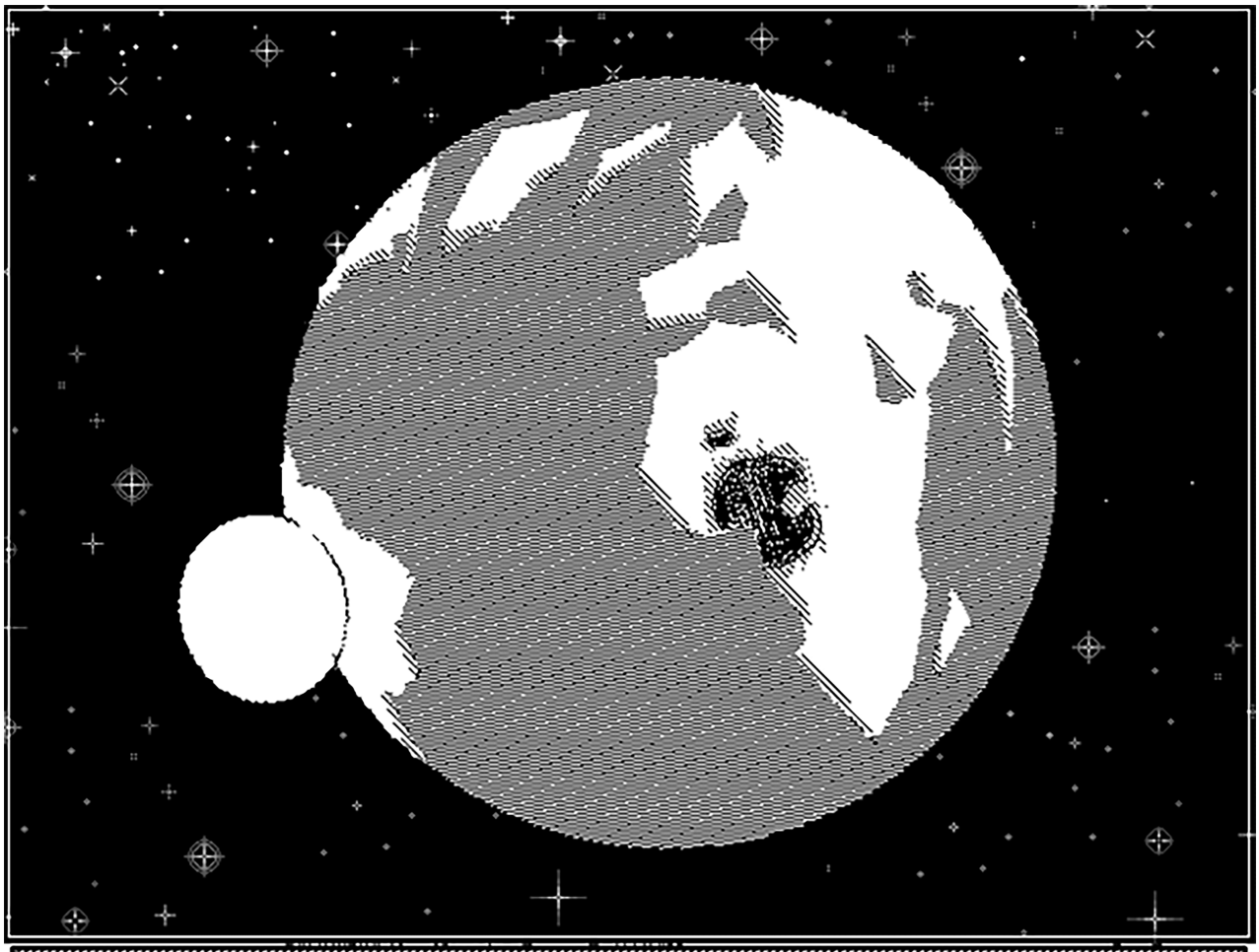
American



```
0   I'm proposing an American
1   Shanzhai culture as an act of
2   resistance. A culture of hacking
3   not for bug bounties but so that
4   we can build our own machines
5   with all the features we like and
6   none of the ones we don't. It
7   will have to remain underground
8   and proof of concept for a while
9   as our government has decided to
10  back Big Tech's ambitions toward
11  monopolization. We'll catch jail
12  time and lawsuits for it if we're
13  not careful. But we need our
14  hackers back on the side of the
15  people.
16  Besides, isn't this how
17  capitalism is supposed to
18  function?
19
..
```

Shanzhai

By gr3ase



```
0   Too much intellectual capital is
1   being funneled into making our
2   machines worse. I'm tired of
3   reading about black hats just
4   trying to score a big paycheck
5   or play war games. We're
6   drowning ourselves in machines
7   which do nothing because rich
8   men profit off bad technology.
9   Bootleg is cool. SHANZHAI is
10  cool. SHANZHAI is the democratic
11  way to create technology that
12  serves the people. Fuck
13  Intellectual Property, embrace
14  technology as a service to the
15  people. Something that solves a
16  problem. Otherwise we're just
17  gonna end up drowning our kids
18  in hot plastic.
19  Know what I mean?          xoxo
```

Refreshments

Interactions

Dear *2600:*

So, this happened the afternoon of August 2nd. It all started at the Grassroots Kava House in downtown St. Petersburg, Florida - once known as "God's waiting room" and now home to young hipsters and developers building what seem to be endless lines of fancy high-rise condos and apartment buildings.

I sat between two guys I didn't know - both seemed to be working. I began talking to the guy on my right after he said "bless you" to someone who sneezed. One thing led to another and the conversation went from the phrase - the origins of which have been forgotten - to Ted Kaczynski to the fact that this guy was a software engineer. He told me that meant he writes apps and programs using Ruby, mostly. From there the conversation went to Linux and Ubuntu and Ubuntu forums and figuring out how to configure a FireWire card in the early 2000s - and I then mentioned I was thinking of going to DefCon the next week in Las Vegas but that the con had become corporate and wasn't the hacker funfest it used to be. He mentioned he had been to HOPE in 2022 and asked if I'd ever heard of *2600 Magazine*. I said of course and that I listened to your radio show, *Off The Hook,* and that I was disappointed I hadn't attended the last HOPE at St. John's University in Queens.

At which point the guy to my left chimed in, "Sorry to interrupt, but I haven't heard anyone mention *2600 Magazine* in a long time." The software engineer on my right then said he still had a subscription to the hardcopy of your magazine.

I mentioned I had just listened to *Off The Hook* on Wednesday, July 26th because I knew your show and the *OTH Overtime* would be about Kevin Mitnick, who had recently passed. I said it was weird because the lead story in the local newspaper (the *Tampa Bay Times)* on July 20th was about Mitnick's death. Mitnick had been the "chief hacking officer" at a Clearwater, Florida security training firm, KnowBe4.

Now, as an aside, I had been looking on your website on July 26th, checking to see which would be the *2600* meeting nearest me. I knew we didn't have one in the Tampa Bay area - and I always wondered why. I read the part about how to start a *2600* meeting, requirements, etc. I had wondered if it would be possible to start a meeting here - but I have almost no contact with any computer types these days, so I kind of shrugged it off.

Meanwhile, both the guy on my right and left were surprised to learn of Mitnick's passing. I asked the guy on my left how he knew of Mitnick and the guy said his job is in network security at a company that has a contract with the Department of Defense for work at MacDill Air Force Base across the bay in Tampa.

So we talked a little bit about that and the origin of our interest in computers and hackers. I told him how, as a journalist, I had written a lot about white collar crime in South Florida and how the story of Kevin Mitnick and some computer hackers got me interested in computers in the mid 1990s.

I also told him that, as a kid, the only hackerish thing my friends and I knew you could do with a payphone was to drop a nickel into the five-cent slot and bang the coin return button as hard as you could with the phone receiver and that sometimes we could make a call for a nickel instead of the normally required ten cents.

I'm rethinking whether there would be enough interest in the Tampa Bay area to begin a *2600* meeting. If you read this far, thank you. Keep up the good work.

gmachine24

Not only did we read this far, but that whole story had us transfixed and filled with hope concerning how easy it is to bring people together. You've proven that and shown how there is indeed great potential for a Tampa Bay meeting simply by finding two random people with such common interests without even trying. We hope others are inspired by this tale. Thanks for sharing it.

Dear *2600:*

Last week I emailed the webmaster and submitted photos of a phone booth. I also called and left a message on the phone number listed at the bottom of the 2600.com web page. Have you replied and I did not receive it (if I am blocked on web) or just arrogant?

Over the past 20 years, I have emailed 2600.com several times, never to receive one peep from you guys/gals. I have been listening to the show off and on from 1991 or so. I would have thought that a simple "hey, thanks" would not be such an effort. In the past few years, I downloaded whole years of show and listened during the day on a USB drive while I travel in my car. I have not listened to this year's shows yet, so if there is trouble at your show, I have not heard about it yet and so, if you are inundated, I do not know about it.

MY

We have been inundated for a very long time. We simply cannot give the kind of attention you're expecting here with the staff that we have. Even massive companies aren't able to do this, though we believe it would be a lot easier for them. But we do pay attention to all of the feedback that comes in from listeners, attendees, and readers. And we are very appreciative of your interest.

Critique

Dear *2600:*

In 40:2, ru0k's critique of DCT's article had flaws. Ru0k defended voluntary collectivism. DCT's collectivism referred to that forced through the barrel of the government's gun. The most extreme form of this was the Soviet Union. Read how well that worked. It's unrelated to the voluntary collectivism ru0k raised, a strawman argument.

DCT's U.S. dollar critique wasn't about "funny

money," but if you want your currency centrally controlled by a handful of unelected bureaucrats or decentralized. Ru0k claimed money is the root of all evil. But without money, there are no price signals to indicate what social needs are being unmet. Without those signals, it is impossible to know what to produce to optimally meet society's needs. The result is universal poverty. Money is the least imperfect means of meeting society's needs. It's not money but seeking to f*** over others that's the root of all evil.

Ru0k misunderstood the vaccine question. It wasn't vaccines good or bad. It was who should make decisions about health protocols at *2600* meetings: decentralized by people running the meetings or centralized by the editors of *2600,* as though a meeting of healthy 20-year-olds in a low-spread county needs the same safety protocols as one with mostly seniors and diabetics in a high-spread county.

Ru0k misrepresented the transgender issue. The threats of violence he or she experienced should be illegal. But then ru0k wrote of those wanting to "limit the existence of trans people" from sports. No one wants to ban transgender people from sports. The concern is sexual dimorphism. Performance-enhancing testicles result in larger bones, greater height, larger lungs and hearts, and other differences that grant lifelong sports advantage. The reason for sex-segregated sports is that if they were integrated, no woman would ever win a championship. In racing and swimming, top U.S. high school boys consistently get faster times than Olympic gold women. Some sports leagues are considering renaming the men's league to the "open league," meaning open to anyone, while the women's league is limited to women who went through performance-diminishing female puberty and don't take testosterone. It's a question of what's fair under biological constraints, not erasure.

Ru0k projects his or her own experience onto all gender dysphoric children. But ru0k's experience isn't the norm. Historic data over many decades show that the vast majority of children grow out of it. Nearly all are gay, often citing internalized homophobia that a man can't be attracted to a man so must become a woman to normalize his sexuality. Look up Corinna Cohn for an example. The issue isn't erasure, but questioning if irreversible surgery and puberty blockers with lifelong health complications is an appropriate treatment for a distress that will fade in the majority of cases.

The problem with politics is that we can share the same values, yet none of us agree how to get there. E.g., I believe the affirmative care model is a net harmful treatment for gender dysphoria; ru0k disagrees even though we both wish for the best treatment and both want transgender people treated with dignity. Or for racism, read the books *Woke Racism* with *How to Be an Anti-Racist*. Or pair *Self-Portrait in Black and White* with *Racism without Racists*. These books all seek to end racism, yet they take incompatible approaches to solving the problem, each side claiming the other promotes racism.

The problem with the politics of culture war is these issues are too complex for anyone to have confidence they know the solution. Thus editorials should be written with the assumption that you're probably wrong. Recognizing this could mean *2600* changing its editorial column to have a diversity of views. Or it could mean stepping away from politics and focusing on shared values. I believe the latter is better, because when we engage in culture war, we forget when we share the same values and end up hating each other. I encourage the staff of *2600* and its readers to read Irshad Manji's book *Don't Label Me* to better understand this point. And I encourage *2600* to review how much of DCT's and ru0k's articles and the editorials DCT complained about had anything to do with hacking systems. I venture to guess close to none.

Stay free. Govern yourself.

DM

We don't have anywhere near enough space to address all of these issues, so we'll only comment on those that directly reference us. While you may believe that editorials which reference events in society or the world are unrelated to the hacker culture, we maintain that there is always a connection of one sort or another which is spelled out in that column. We always encourage readers to think for themselves, but if we have an opportunity to present facts in a way that's relevant to our community in words that no one else is using, then we will take that opportunity. As you know, not everyone agrees, and we give those people their say too. We're encouraged by the amount of interest people show towards issues that we believe are quite relevant and which far too many people ignore and leave for others to decide upon. We want to see the intelligent people in the hacker world get involved in addressing the many problems of the actual world. To get there, we have to engage and listen, often to views we don't agree with. Learning to argue one's position in a respectful and convincing manner is one of the greatest advantages we can achieve.

Regarding our policy with meetings and vaccines, we believe that was handled in as responsible a manner as possible. What you seem to propose would have been to have each meeting decide if they were healthy enough to ignore safety protocols. Nobody was equipped to make that sort of decision with the knowledge that we had at the time. The only way to handle the situation was with an abundance of caution and in a uniform manner that was easy to understand. Nobody stood in the way of people doing whatever they wanted if they felt strongly about gathering. But those were our conditions for having meetings affiliated with us. If you want to say we were too cautious, go ahead. That's far better than not being cautious enough and potentially losing people. Please remember: well over a million people in the United States died from COVID-19 and seven million globally. While mistakes were made and scientists didn't always have the facts right, that's how science tends to work and we all just have to do the best we can with what we have. We're proud that so many in our community did exactly that and we only wish that more people followed the science and not the politics.

Dear *2600:*

Greetings. I've been a customer since the early 90s. I always liked your zine because of its focus area on tech - particularly the tech underbelly that not everyone talks about.

You have an admin on your Facebook group who literally posts pictures of wooden dick statues and who bans people for asking who cares or what the point of the post is.

Just thought you should know who you have representing you these days.

I'll keep the subs coming and attending local meetings. You might want to curate your admins some.

M

We honestly don't know why Facebook makes people act this way and we don't even know which Facebook group this is. (We have three at last count.) We have gotten compliments and condemnations for all of them. As with our IRC network, we can't guarantee that everyone who finds themselves with admin powers is going to act in a mature manner. The words, posts, and actions do not necessarily represent us, but are generated by other readers of the magazine who are putting in some extra effort to run these forums. We have had little interest in Facebook since well before it was fashionable to admit this. But we do respect those who are trying to build a community there. And while occasionally we're hit with a campaign to eliminate or discipline an admin somewhere, invariably we get a counter-campaign to do the opposite. If we spent our time being judges on these disagreements, we wouldn't have time to work on the magazine. So we truly hope these little environments can figure out ways to self-govern and encourage participation.

Dear *2600*:

I hate Sheep. You are a Sheep. Sheep are evil. Ergo, I hate You because you are an evil Sheep!

The Logical Robot

Definitely logical. And at least we get a capital letter.

Dear *2600:*

Two months ago, I resubscribed to your magazine after a very long hiatus indeed. It's been a long time since I had an article published (about 30 years), but in the meantime I've kept an active interest in the hacker world, albeit from arms length; the hacker gene doesn't ever go away. The 40 year anniversary issue has been sitting in my bathroom for a while, and it took me until today to discover the article with "holistic" in the title (my bowels aren't as regular as they used to be). "Holistic" is a useful keyword that usually indicates some prime-grade horseshit is soon to follow, and you didn't let me down. There was a note at the beginning where the editors attempted to distance themselves from the content, but nonetheless I was genuinely surprised you printed it. It's essentially a three page rant from someone who clearly has mental health problems. It led me to wonder how far you would go in the name of freedom of speech. For example, if he had expounded on the conspiracy theories he proudly embraced, how much would you have printed? You mentioned editing certain types of information out already (which I'm sure will have made him think you're working for George Soros or something batty like that), but he still managed to attack "equality" and "inclusion" - a clear dog whistle for the racists and nutjobs out there. Did you have to edit anything out about the Jewish conspiracy or chemtrails?

The funniest thing was how he went on about getting politics out of the magazine - in one of the most political rage pieces you've ever printed.

There's so much more to say on this, but so little point saying it, I'll end here.

Veg

You may not realize it, but you make some good points as to why we printed that article. Freedom of speech is really important and if we can't defend ourselves without accusing someone of being mentally ill or racist, then we're not really presenting a decent argument. We were happy to see people responding to this piece and finding their voice in the process. While it's not the main subject matter of our magazine, such content is certainly relevant to all of us and our opinions should never be stifled. Nor should the discussion.

Dear *2600*:

My eyesight is so terrible on a regular basis that I have the last three issues of *2600* that I can't even read. It really sucks.

Nicholas

Fortunately we now have digital subscriptions and digital access to previous years where you can change the size of the type! People have been complaining about our microscopic print from the beginning, so we're thrilled we can finally provide a solution.

Interesting Findings

Dear *2600:*

First, huge fan, been reading your magazine for years. Thank you for all you do and the hard work everyone puts into it.

This is going to sound crazy, but I was watching reruns of *M*A*S*H* today and noticed something kinda cool. In Season 5, Episode 2 ("Margaret's Engagement"), about one minute into the episode Radar O'Reilly answers a phone call from Tokyo. He says, "I can't hear you, hold on," and proceeds to whistle into the microphone and then says "Sorry, it clears the static." *What?!* Out of curiosity, I pulled up a frequency analyzer app on my phone (not the best app, but it works for what I need it to), and replayed it. His whistle was very, very close to 2600 and peaked at 2900! Am I crazy?

From what I could find, this episode aired in September of 1976.

Kent

You may have discovered the influence of someone in Hollywood with phone phreak knowledge who wound up making the script a bit more interesting. We're certain there are many other such examples all over the place and we hope more readers can share them with us. (For what it's worth, it's unlikely that Radar would have cleared the static by doing this, but may have actually wound up disconnecting the call. Of course, that may have been his objective....)

Dear *2600:*

The researchers at Netenrich have uncovered a promising new artificial intelligence tool called "FraudGPT." This AI bot was built specifically for malicious activities, including sending spear phishing emails, developing cracking tools, doing carding, etc. A subscription is the primary means of payment for FraudGPT. Monthly subscriptions cost $200, while annual memberships cost $1,700.

Ryan

This has been known about since last July. Like any bit of technology, artificial intelligence can be used for good or for evil. We're fascinated by the evil in this case. This should come as a real wakeup call to those who think that setting rules and passing legislation is going to keep everything under control. It won't. AI that doesn't play by the rules is something we're all going to have to deal with. For now, our main goal is to figure out how to defraud the fraudsters so we can play with this thing without having to pay them.

Dear *2600:*

I found this legacy link from 1997 on your site today. Not sure if you're aware that it's open to the public or not, but I figured I'd give you a heads up.

Very neat piece of nostalgia, and the clones of ValueJet's websites are still live.

www.2600.com/hackedphiles/value_jet/

All the love!

Cody

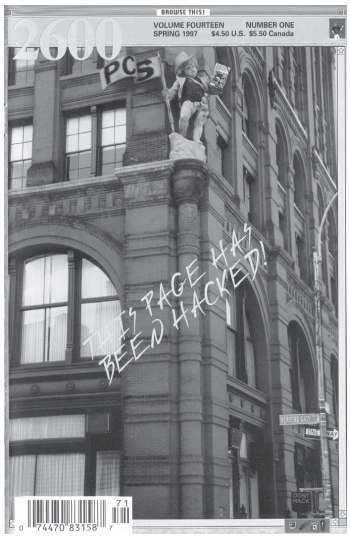
Not the neatest relic out there, but we do tend to hold onto all of our past projects, so they emerge every now and then and surprise us. Thanks for sharing.

Dear *2600:*

I took a photo of 14:1 and submitted it to Bing AI. This is the result: "It's a photo of a puzzle box with a picture of a red brick building on it. The puzzle is 2600 pieces and the box is white with a blue label on the top left corner that reads "Clementoni." The picture on the box is of a red brick building with a green awning and a statue of a man on the top right corner. The building has a sign that reads "The Eagle has been kicked."

Pretty close, eh?

xcm



About the only thing Bing got right was that there was a building with a statue in the picture.

Here is the actual description from Volume 14 of The Hacker Digest: *"Spring 1997 was an image within a browser. The title of the "web page" was "Browse This!" with the masthead info directly below where a menu bar would normally be if this were actually a web browser. Somehow our slogan ("The Hacker Quarterly") was left out. To the right, where a browser graphic would normally be found, was a small image of the recurring hacker that had been seen in various other past covers. The main image of the page shows a view of the Puck Building in downtown New York City, the site of the upcoming Beyond Hope conference. However, a few liberties were taken with the image. For one thing, the words "THIS PAGE HAS BEEN HACKED!" are scrawled across it, a reference to the many web page hacks that were going on at the time. The statue of Shakespeare's Puck - a staple of the building - was altered to have him wearing a* 2600 *shirt, holding a copy of the Spring 1996 issue, and grasping a flag that says "PCS." (PCS phones were making their debut in the States at around this time, using both CDMA and GSM technology.) At street level, Mulberry Street was relabeled as Heavens Gate Way, a reference to the Heaven's Gate cult, a group of web developers who had recently committed mass suicide in anticipation of the arrival of the Hale-Bopp comet. At the very bottom of the page (below the modified "Don't Walk" sign that was made to say "Don't Hack"), some pictography can be found using tiny icons to say that the combination of computers, a comet, and pills will lead to a casket."*

That's a pretty typical description of a cover that's part of the extras of The Hacker Digest *collection. And you could not have a starker contrast between the informed and the uninformed. Bing AI has a lot of work to do. (Since this page isn't in color, we suggest visiting the image for the Spring 1997 back issue at 2600.store to truly appreciate it.)*

Clementoni?

Dear *2600:*

Just found this site with all the Radio Shack Catalogs. www.radioshackcatalogs.com/index.htm

Rory

And just like that, we lost an entire weekend.

Dear *2600:*

It's satisfying to have Verizon FIOS turn on IPv6 and you get a 2600:: address.

Hank

And not at all ironic.

Dear *2600:*

If I ever suffer from a bit of imposter syndrome, I can look back at the time that Google Mail sorted a failure message from its own mailer daemon into the spam folder.

Joel

We've said it before and we'll say it again: Gmail has the absolute worst spam filter. Its over-aggressiveness results in a massive amount of legitimate mail being lost due to their algorithms. If you have a Gmail account, we guarantee you will find legitimate mail in your spam box if you look. You should not have to change the way you speak or

any other individual habits to suit their parameters. Spam filters need to be user-configurable and not dependent on some company's idea on what's acceptable.

Dear *2600:*

On the September 20, 2023 show, the *Off The Hook* cast discussed how Google has a problem with marking too much incoming email as spam. I find that ironic, because when I check my non-Google junk folder, a good chunk of my spam folder is messages from [random letters and numbers]@gmail.com.

I've been self-hosting my email for a long time, so I'm no stranger to receiving spam, but I have seen a noticeable uptick in spam messages from Gmail accounts. Perhaps Google should point their overzealous spam filters at outgoing messages, too!

Colin Cogle

We probably get more spam from Gmail than from any other source. But at least we have the freedom to define it as such on our end. Gmail users are much more likely to lose mail due to an algorithmic change that nobody ever tells them about.

Dear *2600:*

I've been reaching out to AT&T customer support over the last few weeks using the online chat feature. During and after the chat, you have an option to download the transcript. Cool, saves me time from screenshotting everything or copying and pasting it somewhere else. When it came time for me to reference back to the transcripts, it was then I realized that AT&T automatically redacts numerical characters at random. For example, in one transcript I downloaded, most of the dollar amounts were redacted. In another transcript I downloaded, all of the dates were redacted. I feel like this was done on purpose to prevent the customer from holding them accountable for the things they promise. Shady stuff. I have never seen any other company do this.

Jeffrey

Never attribute to malice what can be explained through incompetence. Remember, this is AT&T.

Meetings

Dear *2600:*

Is there a local meeting for Las Vegas?

Frank

There has been in the past but we're not aware of one at present. That is easily solved if one or two people put in a little effort and follow the meeting guidelines linked to at 2600.com/meetings.

Dear *2600:*

I'm interested in finding people locally to discuss security and would like more information on how the meetings process works. I'm a cybersecurity student as of a year now and am very interested in being part of a community of like-minded individuals. I have made it into an honor society, but am seldom able to find someone in my field. I live in Portland, Oregon and see that there is a *2600* meeting here. Any information on this would appreciated.

Joseph

All you need to do is show up. While we can't guarantee you'll find people in your field, we think it's a relatively safe bet that you'll encounter others who take an interest and have some understanding of what you're pursuing. The meetings are always changing and what's true one month may not be the next. But they become all the better when attendees are open to meeting new people and learning new things.

Dear *2600:*

The Stockholm, Sweden meeting is steady, the venue is much liked, and we are about five to eight people each meeting. The interesting thing is that with every meeting someone new joins. Some of the new ones never come back, some do. Our meeting is basically just a bunch of people sitting and talking about work, hacking, tech, and learning languages. We've attracted three hackers from the U.S. who all found the meeting via the magazine. We also have attracted a bunch of ex-pat students, so almost always the meeting is in English. I've managed to get two of my workmates to be regular and two more to come sporadically.

I honestly look forward to every meeting. It's so much more an enjoyment than a chore.

We have a Mastodon account @2600stockholm@mastodon.social which has like one tenth as many followers as our Twitter/X account, but I see three times more engagement on the Mastodon posts.

Another cool thing is that one of our ex-pat meeting goers managed to land her first job in Sweden via help from several of us at the meeting.

/Psychad

This is about as good as we could expect a meeting to be. Please keep it up. We hope many others are inspired by this.

Dear *2600:*

At the last scheduled meeting time, we attempted to attend the Calgary *2600* meeting in the food court of Eau Claire Market listed on your website. However, it didn't appear as though anyone actually met there. Is it possible for you to contact them and see if they're still active and, if so, where they're meeting or how to get in contact with them?

Calgary Hacks

This is unfortunate if true, as it's the only meeting currently in Canada. We don't know why Canadian meetings haven't bounced back like so many others have. We hope to see this change soon, but if we get any more reports like this, we will have to delist this one. We don't share contact info, which is why we encourage meetings to have a social media presence so new people can make contact.

Dear *2600:*

Hi! Lovely to see my photo in 40:2, but in the Meetings area, "Buenos Aires" lacks the final "s." ("Buenos Aire" is printed.)

Arturo 'Buanzo' Busleiman

We are both horrified and pleased at this, as it's a terrible error, but we can always count on our readers to find them. This one ran in our pages for a year.

Dear *2600:*

The Madrid meetings are going well, but we were wondering if you guys can add our email so people can ask questions or our URL? 2600@hispagatos.org or https://2600.madrid.

Happy Hacking!

ReK2

We currently list Twitter IDs on the meetings page (printed and online), but we would like to also include websites. Most meetings don't seem to have these, however. As we don't give out contact info, having a way of communicating with future attendees or disseminating relevant info would be a very good idea.

Dear *2600:*

All of the Milford, New Hampshire meetings have been going well. We have had visitors travel from out-of-state to join us, which has been exciting!

Hope all the other meetings went great too! Thanks again for all you do!

killab33z

We're thrilled to hear this and hope more people stop by.

Dear *2600:*

Hello!

I'm a Colorado Springs native and I was curious what I need to be able to attend the local *2600* meeting in Denver. Thanks!

Sean

You don't need anything other than a will to be there and the ability to get there. The meeting guidelines are linked to on the 2600.com/meetings page and they tell you pretty much everything you need to know.

Dear *2600:*

We had our first meeting tonight at Piccadilly Tap in Manchester, United Kingdom.

Great first meeting, with fantastic representation from women, students, and security consultants to vCISOs. We had maybe 25 people over the course of four hours. We are still looking at venue choices as it was quite noisy at times, and the venue wouldn't be appropriate for someone in a wheelchair.

Rosie & Saskia

For now we will list it at this venue. Please let us know if and when that changes and we'll get it updated. Congrats!

Suspicion

Dear *2600:*

What's up with those purple street lights in the U.S.? I looked it up and found a *Business Insider* article that was very bad:

"Vancouver has spent the past few years switching from old sodium-vapor streetlights to LEDs. The new bulbs, basically arrays of computer chips that convert electricity to light..."

Really? Computer chips? Whoever wrote this doesn't know the difference between a light emitting diode and an IC. Then the article seems to start beating around the bush, explaining the history of lighting for the past 500 years. Not very helpful, at least for me. Anyways, after all the filler, the article seems to indicate the purply glow is due to cheap-ass LED street lights that turn full purple rain when heat damaged. And on a side note, one Reddit user in the conspiracy community had this to say:

"Look up 'How LEDs are made.' Look up the Moderna mRNA therapeutic 'vaccine' under U.S. Patent #10,703,789. It contains Luminol and Luciferase which are both bio-luminescent (glows under UV lights). With enough Luciferase in you (booster shots), a camera sensor could easily detect who in the vehicle is 'vaccinated' and who isn't." (I've not bothered to fact check these claims.)

What do you at *2600* think? Maybe I'm just being an old git. Or is the purple beam down to 5G technology and diffused lasers?

luRaichu

You're asking us if street lights are being designed to keep track of who has been vaccinated while driving in a car. The amount of coordination and planning that people assume exists when there's some sort of an evil plot always seem to far exceed anything that has ever been achieved before. What we are left with are people convinced that every new development in technology is part of some master plan, but they never seem to have any idea what this master plan actually is. We're just supposed to live in fear and suspicion of science, as well as anything new. So here's what we have to say on these points: vaccines are a great way to avoid deadly diseases and they have saved many millions of lives; LED streetlights can sometimes be too bright and don't get fixed quickly enough when they malfunction; 5G has been a big disappointment as it doesn't seem to be as much of an improvement over 4G as we had been led to believe. We're certain these words will ensure that we become defined as part of whatever this conspiracy is.

Tale of Woe

Dear *2600*:

I've read *2600* since the 80s - when I could find it. Though I'd considered writing many times, I never felt anyone would care about anything I had to say. But I've come into a rather lucky instance by which I can read, and re-read, them all. And in doing so, I read a letter in issue 36:2 from Bill that has made me feel I should write.

Like many other readers, I am currently incarcerated. Though every lawyer agrees that I am here illegally, they won't help without money (and lots of it). But whenever I do have an attorney, they don't do anything but take my money. My case has so many holes that you could drive comfortably through it. But no one tries to fight. They start to, then step back, and I get more punishment. Right now I am here on violation, the violation being that I would not admit to crimes I did not do, but probation "felt" I did. I am trying to fight to get back to my family, but I'm not a lawyer, and at 27 cents an hour, I can't afford one.

So what does this have to do with Bill's letter? In the original search of my home, many items were taken including, of course, my computer as well as those of my wife and daughters. The Secret Service went through them and since "they didn't do it right," the local police did (one of the holes). But after I was sentenced, all of my things (computers, CDs, DVDs, etc.) were given to the FBI.

My wife tried to get backups of the hard drives and some of the CDs and DVDs back, as they contained family photos and home movies. While the FBI agreed that the files are of no importance to them, they would not return them.

According to the U.S. Supreme Court, any electronic media (including emails and specific files) are to be returned if there is no current investigation that requires the information and the files are not evidence in a case. Yet the FBI will not return even my daughter's computer, which had no network connection and only had child games like *Reader Rabbit*, *Barney*, and *Barbie*. Their reason? They are keeping them under national security per the Patriot Act because I worked at the CIA and could have hidden information on them (another hole that started it all).

I just want to get my family's videos and pictures back. Why is the movie of the birth of my daughter "national security?" I also want to go home to my family where I belong (the guideline for the violation was extended probation - I was given 6.5 years in prison).

The Patriot Act was great on paper. But it allows agencies too much power to do what they want and then hide behind the law. There should be some kind of accountability.

If any of your readers can help me and my family get our things back, please give them my info or let me know how to contact them. If I was outside, I'd have money and access to resources to fight, but in probation's "opinion," I am better off here (while my family suffers).

Thank you for having such a great magazine and for always being there. You are one constant in my life I'd hate to lose. Sorry I couldn't send this typed or through email.

Tarsk

We're always sorry to hear of anyone going through such torture. While it's unlikely we can do much more than offer sympathy and a means of sharing this story, this experience may help others to realize yet another reason why making backups is so important. Natural disasters and equipment failures are common enough, but having overzealous authorities take your personal data is also a risk, however small we think it might be. It is vital that such backups be kept somewhere else since they're useless if also affected by whatever compromises the originals. We hope you get your stuff back along with your life.

Appreciation

Dear *2600:*

Thank you all for all the hard work you do for our community. This is my fourth decade of being a reader, and I cannot imagine a world without *2600* - but it would certainly be darker and less fun. Thank you all for what you do!

Allen

This is the highest praise we can hope to achieve. Thank you.

Dear *2600:*

Love your work! Finally I can get the PDF version for lifetime! Thank you for showing up on Amazon when you did, otherwise I'd never have a chance to read this.

MTM

It's been a struggle but we're happy to have made it.

Dear *2600:*

Thanks for offering this option to support *2600*. I'm a Kindle Unlimited subscriber, but want to provide my direct support to you. Thanks for the excellent content!

James

We don't know how this whole Kindle Unlimited thing will wind up working, but it probably can't hurt to also read our issue there if you have that service. Thanks for your support.

Dear *2600*:

As a long time subscriber, I'd just like to compliment you on the excellent job you've done reproducing older back issues for sale. I recently ordered the entire set for 1986 and they arrived quickly and in excellent condition. What a blast from the past! 1986 is my birth year and I wanted to read what topics were being discussed back then. I particularly enjoyed the various lists of old phone numbers you had collected. Very cool. Keep up the great work and a special thanks for working with those who are currently incarcerated.

Also, I'd like to know if *2600* readers could shed some light on software or hardware hacks or workarounds for the JP5 tablet from JPay. Note: Triple-tapping the build number in Settings reveals an applications listing showing each app's software version and Android file names. Hope this helps!

Vincent

We'll leave that to our readers to analyze. And while we no longer have 1986 back issues in printed form, they do exist digitally and in really good quality.

Responses

Dear *2600:*

This is in response to 39:1 on page 39 by Snake in a Lawn Mower: Using trial and error with the reader mode using Safari and Firefox yielded a few other findings for me that I wanted to share. First, as of this writing, *The New York Times* is still readable with this hack, plus *The Christian Science Monitor* can also be read, and this appears to work for *The Washington Post* too.

However, this reader mode wall hack-around works not just for paywalls on certain sites, but also on bypassing cookie walls too, which seem to have started becoming a greater annoyance popping up at a greater rate. It can also work on getting around on age-consent walls on certain blog sites for reading certain articles.

If these walls are giving you trouble in accessing information you want, be it cookie walls, certain paywalls, or consent walls (at least so far for blog sites), try reader mode as a potential option.

Mx. Blu3

We do want to make sure these publications are supported and continue to survive, as their existence is hugely important to a free society. But finding ways around restrictions is what we do, so we intend to continue pointing those out when we find them. Walls are meant to be breached, after all. But we'd also like to use our creativity to find better ways of supporting publications, journalists, writers, etc. because the current system tends to benefit the wrong people.

Dear *2600*:

The following is a response to the article "Friendly Fraud" in 39:4. I wanted to elaborate on some basic ideas of banking. To start, our monetary system is based on fiat currency, not money. The main characteristic of money, and not currency, is it has to be a store of value over a very long period of time. Fiat currency does not do that, and all the thousands of fiat currencies eventually have no value. The USD is currently on this decline.

So banks are not in the business of protecting your currency. They are in the business of lending your currency. Because they are subject to currency devaluation (inflation), just like you and me, they have to lend out your currency at a higher interest rate than they are paying you, currently less than one percent. Banks used to give an interest rate to savings accounts and certificates of deposit because the bank customer was taking a risk in lending money to the bank. To reward this risk, let's say they paid you five percent.

When you put cash into the bank or transfer numbers from one screen to another, that currency really isn't yours anymore. It is immediately lent out by the bank so they can make gains. But why do you still "see" your balance on your statement? The bank has imaginary currency called bank reserves, which conveniently are denominated in dollars. So even though your statement might say you have $1000 in the bank, in reality, there is no cash in the bank at all. When you withdraw that $1000, you are not getting "your" currency back, you are getting back someone else's $1000. But, you don't care which dollar bills you get back, as long as it adds up to $1000 though, right?

So, when we think the bank is required to "keep your money safe," it is not. The bank is only required to put a placeholder, denominated in bank reserve dollars (imaginary currency), so you retain confidence in that bank and keep depositing currency units there. Banks today are actually not even required to keep much physical cash in the bank anymore. You can read about historic bank runs throughout history.

On a more philosophical note, when banks are very supportive of the customer and take their side when charges are disputed, you are also assuming they actually have cash sitting around they can refund customers with. The bank literally takes no risk when it lends out your currency because you literally gave them the deposit to lend out, and you aren't even making any interest on it. You're only getting the false sense of security that your dollars are actually physically in the bank, which they aren't. When the bank disputes a charge, it draws on lines of credit, or the merchant will draw on a line of credit and refund numbers back to your account. The real losers when fraud like this happen are the individual small business owners. These businesses lose time, labor, and capital when physical items get refunded or someone frauds them somehow. Banks and credit card companies literally have no "skin in the game" and it's always the small business owners who get hurt the most.

The article states the bank has to insure you up to a certain dollar amount. This is done with the FDIC, one of the more interesting Ponzi schemes from our former socialist president: FDR. The government will "insure" deposits up to $250,000. When the government offers insurance, protection, or a bailout of any kind, just like individual banks, they can create currency out of nothing and transfer it to the unfortunate customer. The only difference is the government cannot create currency itself. The Federal Reserve (a private company) has to create the currency from its imaginary account, then lend those dollars to the Treasury, or government entity, at interest, and finally those dollars trickle down to "save" the bank customer's deposit. All this does is encourage banks to lend more recklessly, because they have a "safety net" with the government. This was demonstrated in the mortgage crisis, when Freddie and Fannie became government entities, literally every time a bank signs a mortgage, when financial firms get bailed out like TARP... the list goes on.

Remember - if anyone wants to commit fraud - the small business owners you might be affecting. But banks, credit companies, and the government all operate on an imaginary system of numbers and accounting entries, not a true monetary system. What is real is our time and labor that we trade in exchange for those currency units. The real fraud is how we continue to let the government devalue everyone's real labor by continually producing new currency, injecting it into the economic system where it goes to people who do not work for that currency. Ask yourself this: If two people have $100, but one of those people worked for that $100 and the other was simply given that $100... whose $100 is actually worth more? Herein lies the great debate of the current rising pricing of everyday services and commodities.

To all the readers of *2600,* I encourage you to explore the YouTube documentary "Hidden Secrets of Money" and watch all ten episodes. This exposes one of the greatest frauds in history, our current monetary system.

I also encourage readers to explore credit concepts as well. People have control over their credit; they are simply not informed. Anyone with an SSN can create three profiles on the credit agency sites and control their own credit. The article oversimplifies "bad" things that can happen to your credit, when in reality your credit is extremely flexible. It's all a bunch of numbers and algorithms anyway, so it's in people's interest to learn how to hack their credit. No one can pull your credit without your consent if you freeze it. Aside from being under some government investigation, no company or individual can touch your credit profile.

I'm always surprised that intelligent people like hackers can waste so much time doing things like trying to fraud banks for pocket knife purchases, sneaker purchases, and whatnot. Take that energy, learn the monetary system, and go start a legitimate business that actually contributes something to society. If anyone needs some guidance in this area,

please feel free to email me at deltacharlie.tech@➥protonmail.com.

Delta Charlie Tango

We always knew our imaginations would serve us one day. We didn't know it would have so much to do with banking.

Dear *2600:*

I assume you're not in the habit of correcting errors of fact in your responses to letters outside of those involving hacker things and maybe some tech aspects, wisely leaving them to your readers. In that case, I have to point out that aestetix makes one historical error, which leads to another bit of sloppy history in his letter in 40:2.

First, the error: Former Fed chairman Paul Volcker was never a close associate of Ayn Rand. aestetix was perhaps confusing him with his successor, Alan Greenspan, who was.

Second, aestetix then says that if the free-market theories Volcker impliedly espoused were so great, why did the economy tank shortly after he took over as Fed chairman? Well, argument by rhetorical question is a very bad idea if you're not completely sure no one can answer it. In this case, the answer is: because that was the point.

Readers old enough may remember that the 1970s were plagued by inflation. Carter appointed Volcker to head the Fed, and Reagan was elected the year afterward, largely to do something about this. What the Fed did was focus on reducing the money supply by raising interest rates sharply. Yes, this did bring about the 1982-83 recession, from which some areas have never recovered. They knew this would happen, but accepted it as a tradeoff for bringing inflation down. When inflation did slow down, this also caused the farm debt crisis and the Third World debt crisis later that decade, as the lending had been based on the idea that inflation would continue for the foreseeable future. By the early 1990s, inflation was almost negligible.

I am not saying this to defend those negative outcomes, which caused a lot of pain. But it is the current accepted consensus of economic historians across the political spectrum. There are debates as to whether it could have been more equitably managed. But it is only fair to the readers of *2600* that we make sure we get all our facts right, in a time when too much bad knowledge is floating around out there.

dcase

This is probably the most we've ever focused on the financial world in these pages. Let's steer in a different direction now.

Dear *2600:*

I just got the new quarterly in the mail and have had a few beers... I may not always agree with what *2600* says, or whatever anyone ever says in general, but I'll defend our right to speak our minds and set information free till they put me underground.

MW

There ya go. That pretty much sums it up.

Dear *2600:*

Thanks to pax for the interesting article entitled "Cute App, But I'll Use My Own" in 40:3.

The obsession with having apps for everything is getting out of hand. I have a phone running Lineage and only use F-Droid as my repository, so I know how irritating it is to be required to use various "apps" to get things done in life.

During the COVID lockdowns here in Victoria, Australia, the government introduced a system where you scanned the QR code at any venue you wished to enter. This was to be able to keep tabs on close contacts when infections occurred at a certain place and also to inform people if they may need to get tested.

The QR code would take you to a government website when you could either download an app or you could enter your details on the website.

While I was a little worried about how the information could be used, COVID was a very extraordinary situation and I strongly supported the Victorian state government's strong handling of the outbreak (although there were some areas where I think they could have done better, but they generally handled it pretty well). As a result, I was prepared to take the potential risk to my privacy, as saving lives was the bigger issue.

I was impressed with the fact that you could fill in your details on the website, as I wasn't required to download and install a proprietary app.

Unfortunately, later on they removed the feature on the website, and then you were just directed to links to Google Play and the Apple App Store, where you could install the app.

For many venues, I would go up and say that I wanted to sign in, but didn't have a smart phone. (I wouldn't bother explaining Lineage or F-Droid as opposed to Google Play. That would just make things complicated. I'd just keep my customized smartphone out of site when talking to them!) I would get funny looks at times, but I usually could sign in with a pen and paper.

However, not all outlets had the pen and paper option, which really annoyed me. I would always be polite to the people I talked to, but would ask them to pass on a complaint that I felt it was discriminatory to those who hadn't bought into Apple or Google's empires and just had an old-fashioned phone. Most people could understand this, but not all.

Interestingly, at one point, I did download the app via different means and had a look at what classes/libraries were included. There are many good programs to do that (for example, "ClassyShark" which is available from F-Droid). I shouldn't have been surprised to find the usual suspect classes and libraries from Google and Adobe which track users. Just further insult to those who want autonomy over their technology!

But what pax describes is totally next level. Needing an app to open a stupid gate is just ridiculous! I'm impressed with pax's solution, but it still begs the question: How do people get in and out when Internet connectivity is down?

It just creates yet another unnecessary reliance on your technology and the Internet all working correctly to get on with daily life - not to forget all those little threats to privacy that add up.

The spirit of hacking encompasses many things,

but a huge, central tenet of hacking is the ability to control your own "things."

All the best.

Chris

That is indeed what it comes down to in the end. The toys are great fun and we all love to play with them. But ultimately, it should be about individual choice and being able to accommodate people who do things differently. That's what makes us all stronger.

Dear *2600*:

This is a response to ThoughtCrimes, page 22 of 37:1. Even if you aren't committing any crimes, we all need to be concerned about Big Brother's outreach. You never know when they will decide that they don't like something you did or said. You *never* want to be on their radar!

Many criminals use prepaid cell phones as burners so government and law enforcement agencies might have an interest in surveilling their use, especially if this carrier in particular is often used by foreigners traveling to the U.S. Perhaps this carrier was entirely set up by the DoD for that purpose or maybe it has ties to them? It's anybody's guess.

Of course, you could always contact their support and ask them; I'd be curious as to what they'd say or if their IP space or Whois info changes suddenly after this is brought to their attention. Regardless, I would likely use the default T-Mobile APN settings, always route through a VPN, and/or just dump that carrier entirely.

Also, in response to Morlock Elloi, page 54 of 37:1, I often wonder why people continue to accept and use these totally centralized systems. You never know who has access to your data, or who will gain access. It is super easy for governments to spy and hackers to steal personal data en masse. The way Internet applications are typically set up is akin to a burglar breaking into a single home and getting away with millions of people's property.

This could be changed if every individual ran their own server(s) or if we abandon the server/client paradigm. The former would be more efficient as the client may not always be online and packets would be discarded.

So why aren't people doing this? There's plenty of great and mostly open source software available to suffice these requirements. I imagine it's mostly due to lack of knowledge and understanding, but also lack of time and resources. They feel more comfortable letting the so-called "experts" handle their data. But these "experts" have security breaches all the time. Even if you are no expert and your system is somewhat shoddy, you would still be less of a target than the big "experts."

As for cryptography, should we follow the experts' suggestions? I'm still not sure. Cryptography is not an easy subject for the average person to fully understand. Perhaps it would be best to mix a well known cipher with your own custom cipher? Or would that compromise the whole system?

Dan N

Unpredictability and a wide variety of individual traits are good ways of keeping from being caught up in massive data breaches. But, as you say, time and resources are major limiting factors for most people. That doesn't mean we can't start changing our habits and learning more about how to run our own systems. There would certainly be lots of mistakes made and poor security choices by some of us. But the targeting would have to be on an individual level rather than on a million or more users who never had a chance to overcome their provider's poor security choices. Any time end users have the opportunity to make their own mistakes and build their own systems, it's a win in the long run. That's what the hacker mindset is all about.

Q&A

Dear *2600:*

Is it possible to get a lifetime digest PDF and lifetime EPUB as a combined item? I see there is the ability to have the double lifetime, which provides PDF annual digests and paper issues going forward. Would this be as simple as purchasing the lifetime EPUB subscription and then purchasing the lifetime digest digital upgrade? The PDF digests and access to all the previous digests is great, but going forward EPUB seems to make more sense for e-reader use.

I've been a reader for many years. I used to buy your magazine in local bookshops here on Long Island and then eventually got a subscription via Amazon Kindle (because it was convenient), but it seems you guys outlast the ever-changing landscape of magazine delivery and I want to keep reading and keep supporting you. I travel a lot for work, so reading on some kind of electronic device is simple, as my new Kindle takes up the same space as only a few issues of your magazine, but I can carry all of them and so much more.

Justin

By the time you read this, we hopefully will have more options available, at least one of which should be helpful for you. The delay was needed so we could make sure there were no hiccups in delivering subscriber issues for our new digital options. Fortunately, there weren't, which opens the door to all kinds of possibilities.

Dear *2600:*

I have a general question regarding private numbers and blocking Caller ID via *67. I remember when Caller ID was being rolled out mainstream, and Ma Bell marketed this service to block your Caller ID from being seen. It was on a per-call basis, so you'd need to dial the prefix before your area code and number to temporarily block your phone number. Caller ID units used to say "PRIVATE" or all dashes. I was under the impression the receiving party would not get the caller's information if they dialed *67. To test this today, I dialed an 800 number inbound to a company I have an existing relationship with. The representative was able to "pull up" my phone number, address, and name. This is despite dialing *67. Do the modern phone systems pull subscriber data regardless of Caller ID displays?

Dave

When you dial a toll-free number such as the 800 number you called, a technology called Automatic Number Identification (ANI) is used rather than

*Caller ID. The *67 option has no effect when calling these numbers. The same thing happens if you call 911. While it's possible to mask your number, it's not nearly as straightforward as with Caller ID. (Incidentally, when Caller ID was introduced, some phone companies only offered per-call blocking where, as described above, you had to dial *67 before every call to block your number. Others offered all-call blocking, which established blocking as your default. *82 was the code to un-block. But some companies used *67 as a toggle for all-call blocking in the early days, leading to customers not knowing if they were blocking or unblocking. Hijinks ensued.)*

It should also be pointed out that other non-800 numbers are also capable of using ANI instead of Caller ID. We've even caught Verizon passing data they shouldn't onto non-ANI-using called parties despite a block being in place. In short, it's not wise to trust Caller ID blocking.

Dear *2600:*

What is the desired length of an article?

Bob

It's different for everyone, but we would like to see more in-depth articles that run a few pages. Short articles are fine too if there isn't a lot of detail to impart. The important thing is to express yourself if you have something to say or share. That's what makes all of this so interesting.

Dear *2600:*

Hi folks, I've got a question on sharing digital editions of *2600*. We've got an InfoSec community at work here in Poland. These are mostly younger folks who likely haven't heard of you. What's your stance/legal approach of copying and distributing *2600* in full or fragments amongst people at work?

Micha

We don't have copy protection or DRM, which means you get to determine what you do with the content. Of course, too much sharing without subscribing and we wind up struggling, so we ask people to be considerate and think of how they can ensure we stick around so we can continue doing this.

Dear *2600:*

I'm in a number of vintage computing groups. There is a common claim that older operating systems are not vulnerable to attacks. I maintain they are very vulnerable. If one were to boot up a Windows 98 machine with vintage browsers and surf the web, would it somehow have defenses because this software is so old as to be no target?

John

There is most definitely a school of thought that believes this. We don't recommend relying on old and outdated software for anything truly important, but we also don't recommend blindly updating every time you're told to. Oftentimes, that's where security problems pop up. In the end, think for yourself, get familiar with firewalls, and keep regular backups.

Dear *2600:*

I'm not much of a hacker, but I had some recent success hacking a Chromebook to run Parrot OS. Now I have a small laptop with a 12-hour battery I can use to learn about cybersecurity and webdev. Any interest in an article/walkthrough on the subject? I'm not sure if it's been covered before. I'm not much of a writer either, but I'll give it a shot.

Professor DOS

That's exactly the spirit we need, as well as the content. We look forward to seeing what you come up with.

Dear *2600:*

One thing I've never quite understood about the 2600 hertz whistle apart from serving as the "aha!" moment... did it have any practical use? What I mean is this: imagine that it's 1967 and you have the whistle. So you pick up a phone, dial a toll free number, and once it connects, blow the tone. OK, so the remote tandem disconnects, and now you're sitting on an open trunk line, ready to accept new instructions. So... now what? You need to be able to generate MF tones in order to make use of the trunk, which means using a blue box. And, if you already have a blue box, then you don't need the whistle, do you? I've never come across any solid evidence that the whistle itself was a useful tool. Stories of it as a physical object involved in the manipulation of the telephone system seem... apocryphal in a way, like the notion of an apple physically hitting Newton on the head.

Joe

For the most part, you're right in that the whistle on its own wasn't all that useful without the blue box, which is what generated the special MF tones. Most blue boxes already had the 2600 hertz tone built in, making the separate whistle redundant. However, it was good for testing without holding a cumbersome box up to the mouthpiece and for showing off in front of friends. Not all connections could be seized in this manner, so this would be a quick and cheap way of finding out.

Dear *2600*:

What happened to www.2600index.info? The last issue to be reviewed here is Autumn 2018. An update is long overdue.

Mr. Nobody

As we've never run that site, we have no control over it. Such projects take a lot of maintenance and this was something that a dedicated reader started. We're happy to spread the word when these types of accomplishments pop up, but we can't be surprised when life gets in the way.

By the way, the latest neat project we've heard of is offthehook.cc, an AI-generated transcript of every episode of "Off The Hook," our weekly radio show. Many thanks to Santiago from Madrid for putting this together.

Dear *2600*:

Any information or methods about how to detect if surveillance software has been surreptitiously installed onto any type of specific device? Personal standalone computer, networked computer, smartphone, iPad, etc., on both a hardline and a wireless Internet connection. Any advice you could provide would be deeply appreciated as one can never be too careful about who's watching you these days.

The Master Cylinder

The thing about surveillance software is that it's designed to be hidden. We could tell you to look out for processes that don't appear to be legitimate or log any and all odd behavior, but oftentimes there are valid explanations. Spyware run by employers can usually be found, but then your efforts at finding it will also be observed by them. We suggest searching online for the latest updates on what to look for. And while we advise people to always assume they're being monitored in some way, that doesn't mean you have to let that change who you are or your overall level of trust. That's how you truly lose your freedom.

Dear *2600*:

My friends and I are having trouble finding an answer to a technology question. I am turning to you as your background and experience in this area make you the most qualified people to provide an intelligent answer. How does device specific electronic surveillance work? This could be electronic surveillance on any type of device: computer, phone, tablet, pad, walkie-talkie, etc. Thanks for any help with this.

P_S_y_c_h_O-pup

There is no one answer to this as all electronic devices are different. A key logger on a computer can be installed remotely or with physical access. A phone can be monitored through the company or via social engineering. Walkie-talkies can simply be listened in on if you're broadcasting on an open frequency with no encryption. The possibilities are close to endless. And we are always interested in articles that go into much greater detail.

Dear *2600*:

I wonder if any of you know of any in-print publications that focus on technical topics like Linux, Windows, servers, application development, etc. I am one of 2.5 million in the U.S. who are *not* allowed to access the Internet. I love reading every issue of *2600*. I also read *Maximum PC* and *Linux Format*. I would get *MSDN Magazine* but it went out of print (digital only) in 2015 or so. Maybe if I had Internet access, I would do a search on DuckDuckGo for magazine or journals in print, but I cannot. Can you help a guy out? Thank you for the great work that you do. Don't let the whiners get you down. HTP.

Looking for Information
(incarcerated)

Some titles we came across were Popular Mechanics, MIT Technology Review, *and* Technowize. *We're certain our readers will come up with more.*

Dear *2600*:

Why not have a column for readers to submit problems and offer solutions? I have two.

Why does my Motorola phone tell me I should use their charger and cord? (Their cord was defective.)

Why do BMW cars not start with non-BMW batteries?

Anonymous

These two issues are related. Companies want you to buy their stuff, not that of their competitors. They try to make you do this even after you've already bought their products. We've seen printer companies try to strong-arm customers into only using their toner, sometimes even making it impossible to use another brand or artificially expiring toner while it's still perfectly fine. There is only one way to deal with this sleazy behavior and that's to help drive these companies out of business. This goes beyond attacks on the right to repair and constitutes a threat to the right to buy.

Moving on Up

Dear *2600:*

Next month will be my first meeting with the organization. I am very excited to interact with you guys! My long-term career goal is to be an ethical hacker.

I did a ten-month boot camp for cybersecurity. I am now working as a PC support tech and my passion has always been the software part. I look forward to interacting and learning more from you.

See you guys soon and thank you for your time.

taddy

We wish you the best and hope things work out. We're not big on labels, the term "ethical hacker," or boot camps. Maybe they work for some, but we believe the real determining factor comes from the individual themselves and whether or not they have the hacker mindset to begin with. With that kind of a foundation, there is much that can be built, but we need to remember that there is no magic formula and that everyone is different. There are many really good hackers who cannot pass these manufactured tests and have little interest in them. Anything that discourages them is not what we want to help promote.

Dear *2600:*

I was a disabled alcoholic for two decades. I had no tech background. Knew how to browse the web and run a torrent on a Mac. I found Linux and began setting up VMs on a cheap desktop machine I bought on SSI. I lived open source as a discipline. If there was a FOSS, yet difficult, way to solve a problem (like streaming, cloud sync, etc.), I forced myself to use it. If there was a better, yet more complicated, way to use my desktop machine, I reinstalled my system. Today, I'm a year into my career as a Linux support analyst. I've never had a CS class. I didn't have any certs before the job. Just go for it. People ask me how to get a job in Linux all the time. Just love Linux. Don't like it. Don't play with it. Don't use it on your *other machine*. If you love it, it can happen. (I use Gentoo, by the way.)

Joe

This is what it's all about. When you realize you have the ability to steer your future, and the desire and passion to learn, that's when the doors really start to open. Thanks for sharing this inspiring tale.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

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

EFFecting Digital Freedom

by Jason Kelley

Against Privacy Nihilism

Maybe it happens when you're explaining the importance of end-to-end encryption to a flummoxed friend or family member. Maybe it's when you're trying to find the "don't share my data" option in a new app, and it's buried so far in the settings menu that you want to scream. Or maybe you found out about something *good* - that a new privacy protection exists, for example - but it feels like a grain of sand in an ocean of dangers, and you still feel completely overwhelmed at what it takes to truly protect your private life from the people, governments, and corporations that seek to invade it.

That feeling of despair - the idea that there's nothing you can truly do to protect privacy, so you may as well throw up your hands - is often called "privacy nihilism." It's summed up in the far-too-popular phrase, "Privacy is dead." Lately, I've seen it tossed around a lot. And I get it; many of us who get this feeling are the ones who care the most about privacy. Sometimes, in my worst moments, I have that feeling, too. But I also know, deep down, that this feeling is flat-out false. Here's why.

You may feel like there's nothing you can do, alone, to move the needle. But you aren't doing it alone. First, remember that the fight for privacy is a collective effort. Organizations like EFF unite tens of thousands of members who care about protecting privacy, and there are many dozens of organizations, maybe hundreds, like ours around the world. We wouldn't all be working together if privacy was already dead. And we aren't the only ones who care: Americans overwhelmingly support new privacy protections, and in general, the country has grown more concerned about how the government uses our data, according to trustworthy surveys.

Maybe you're feeling despair because there aren't more comprehensive privacy laws in the U.S., and it may feel like we will never get them. Well, I am upset too, but there is definitely progress in the laws. Just as one example - the California Consumer Privacy Act of 2018 granted important rights for Californians, and this year's DELETE Act made it even more effective. Soon, anyone in California will be able to easily opt-out of data collection for many data brokers, and delete the data collected about them as well. This is just one step in the fight, but it's an important one.

Change takes time, and the journey to comprehensive privacy protections is a marathon, not a sprint. Today we take many privacy protections for granted, and often assume that things are only getting worse, not better. But many important rights are relatively new. Legal victories like the Supreme Court ruling in *Carpenter v. United States,* requiring warrants to obtain cell phone location data, are evidence of this real, crucial progress. The fight is long, and we know that.

Some of the progress is technical, not legal. The widespread adoption of the HTTPS protocol for web encryption is a significant win for online security and privacy. Achieved in basically under a decade, this shift highlights the effectiveness of concerted efforts to create and spread privacy-preserving technology. The evolution of privacy tools is also real progress, and worth celebrating. We've gone from complex methods of private communication like PGP and GPG to user-friendly options like Signal and WhatsApp, which many more people can (and do) use. There are many, many other examples: the Tor Browser offers fairly simple anonymous browsing and routes around censorship; password managers protect your passwords and your accounts; third-party cookie blockers like Privacy Badger stop third-party tracking. These tools all push the needle forward, sometimes in place of strong privacy laws, but often, as part of a concerted effort to get us there.

In truth, most of us still have rich private lives, primarily free from government surveillance, and most of us can choose not to allow corporate surveillance into those lives as well. Yes, there are certainly spaces where privacy is in danger, and there are some communities who have far fewer privacy protections than others. This is absolutely a problem we must solve. But we are working to improve it, and the awareness of it is part of the process - knowing where those less private spaces are, and who has less privacy, helps us all take precautions to defend ourselves.

Our advice when you're feeling nihilistic? Be practical: use threat modeling - the practice of identifying specific threats to your privacy and taking concrete, practical steps to protect yourself. Figure out what threats you specifically should worry about. Next, stay informed and involved: engage with privacy initiatives where you can, and participate in the ongoing conversation about digital privacy. EFF is constantly offering ways for you to make your voice heard, and to spread awareness.

Maybe you've never had that feeling of despair. That's great. Hold onto this in case you ever do, or just to share with others as a reminder. It can feel overwhelming to care about something when it feels like a losing battle. But we aren't losing. We're just learning to create the better future that we want to see every day, together.

We wouldn't do all this work if we thought the death of privacy was inevitable. Of course, our success isn't inevitable either - it takes real work, and we hope you'll help us do that work by joining us. Take action when you can. Teach a friend who wants to learn more. Become an EFF member to power us through the next big legal battle, activism campaign, or tech project. Giving up is exactly what many government officials, law enforcement agencies, big tech companies, and other powerful people want. Our movement is not a pessimistic one, even if the fight is difficult. It's celebratory. Don't let the privacy nihilists into your head, or your laptop - put a big EFF sticker there instead.

Quantum Computer Algorithms,
Part III: DES Decryption

by Dave D'Rave

Earlier in this series, we discussed oracle-type quantum algorithms. In this article, we look at using an oracle algorithm to perform a known-plaintext attack on the DES block cipher systems. (DES is a well-known crypto system. Wikipedia has several articles on it.)

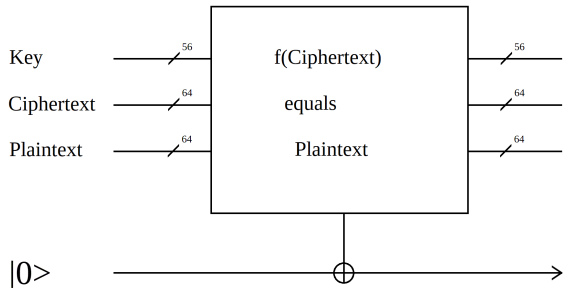
Mainstream block cipher systems, such as DES or AES, break long messages up into fixed-size chunks and then encrypt each block individually. The usual procedure is that the first block is encoded with the main key, and that all subsequent blocks are encoded using an incrementing key, or some combination of the previous blocks (block chaining). The situation is that if you can break the first block and recover the key, then you can break the entire message with very little additional effort.

Known Plaintext Attack

It often happens that we have intercepted the ciphertext and we have also obtained the plaintext. This is sometimes as simple as knowing that the message always starts with a date. The history of cryptography is full of examples of how plaintext was acquired.

The central idea is that, once you have known plaintext, you can build an oracle which accepts a key, the ciphertext, and the plaintext, and which outputs a single bit. The output is |1> if the input ciphertext decoded by the key is equal to the plaintext, and |0> otherwise.

For example, the DES block cipher uses 64-bit text blocks and a 56-bit key. The "good plaintext" oracle for DES accepts the 184 bits of input and outputs one bit. The DES oracle is:

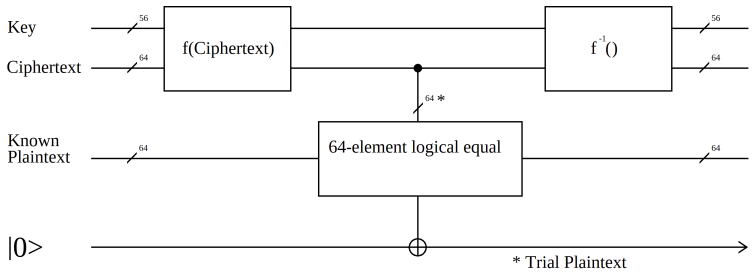


The DES Oracle

The DES oracle is made of smaller blocks. These are the decrypt block, the inverse decrypt block, and the compare block. The inverse decrypt block (f^{-1}) is used to prevent noise errors from back-propagating into the output. Current technology requires that we use this block.

The decrypt block accepts a 64-bit ciphertext input and a 56-bit key input. It produces a 64-bit trial plaintext output. The compare block accepts a 64-bit trial plaintext input and a 64-bit known plaintext input. It produces a single bit output, which drives the output CNOT.

Note that the ciphertext and known plaintext are classical data, while the key, the trial plaintext, and the output are qubit data. If you provide a superposition as the key input, then the output will often be a superposition. This fact is useful.



f(Ciphertext): The Quantum DES Decrypt Block

The algorithm for DES is widely available. It is usually written in C, and is usually implemented as some mixture of for() loops and table lookups. The usual procedure is to first "unroll" the loops, which is a standard computer science operation, and then test that the algorithm still works. Next, either run the unrolled version of the decryption algorithm through your quantum compiler, or run it through a convert-to-Qiskit program. At that point, you should have working code, and can run it when a suitable quantum computer becomes available. In the year 2029.

The unrolled algorithm for DES has 16 rounds of bit scrambling. Each round takes some function of the 64-bit intermediate ciphertext and some bit function of the key and then performs an exclusive-or. This requires something like 120 two-input quantum gates to make up the key function and text function, along with something like another 64 gates for the actual XOR. Note that XOR is implemented by the quantum gate operator CNOT.

As a practical matter, you will need support gates and ancillae, so each round is going to cost maybe 250 gates. Given that we need 16 rounds, this is going to be 4000 gates. Because of phase noise effects, a practical system also needs an inverse DES block. The total adds up to 8000 gates.

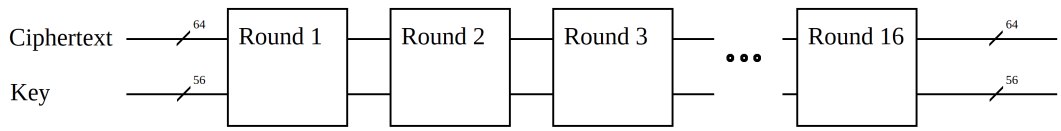
The DES Decrypt Block, in Detail

The DES block consists of 16 sub-blocks called rounds. The traditional (1970s) implementation uses the same code for each

round, and customizes their behavior using what are called "subkeys." At this time, a quantum algorithm probably will use 16 slightly different rounds in order to reduce the total number of quantum gates which are needed.

Optimization methods, which hopefully speed things up, are discussed below.

(The technical reasons for this procedure involve the fact that early DES implementations used either 8-bit microprocessors or dedicated LSI hardware. The obvious way to do the software was to pre-compute the subkeys and then use 16 identical rounds, each with a different subkey. The obvious way to build a DES chip was to only have one round implementation and use it multiple times, with slightly different control inputs. In the quantum world, memory devices are a source of error. A straight pass-through design uses more gates but less memory, so it is preferred.)

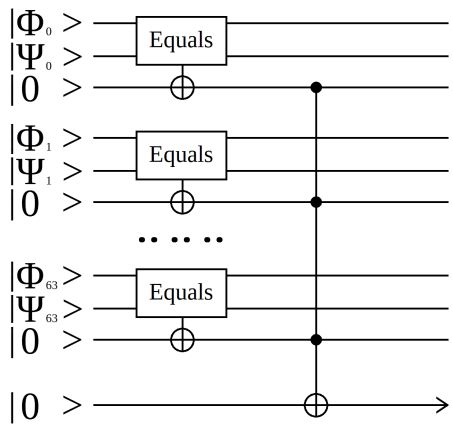


The Inverse DES decrypt block is the same thing, except in reverse.

The Compare Block

The 64-bit compare consists of 64 one-bit compare operations followed by a large AND gate. Each of the input bit pairs is individually compared, starting with the bit 0 pair and moving to the bit 63 pair. The AND gate is implemented as a 64-controlled NOT gate.

Because the 64-input CNOT gate is likely to be implemented as a funnel of two-input CNOT gates, the total compare block consumes a rather large amount of gate resources.



Superposition and Parallel Processing

In order to achieve substantial speed improvements, quantum computers use superposition. For example, we could provide a key value of |all keys whose high-order 48 bits are zero> as inputs to a quantum DES algorithm. This input set contains a superposition of 256 keys.

If none of the keys provide a valid decode of the cyphertext, then the output will be a pure |0> state. If one (and only one) of the keys is valid, then the output will be approximately k*(16*|0> + |1>). As a practical matter, amplitude amplification methods are then used to produce a clean |0> or |1> output.

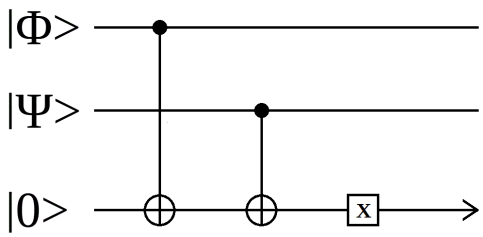
Depending on the noise characteristics of the quantum computer hardware, some kind of bisection algorithm or subset algorithm will be used to pick off the value of the individual key bits. Ideally, this is done one bit at a time, which means that 56 iterations of the DES algorithm will be needed to break a given message.

Tech Notes: Optimization Methods

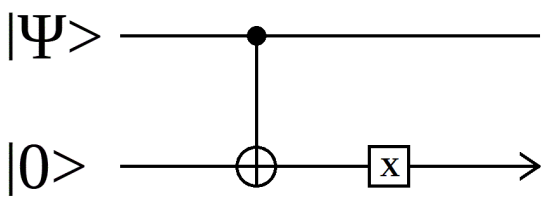
All of the better quantum compilers include obvious optimizations, such as |X|X| equals |I|, or "if you see two NOT operators, remove them both."

This particular algorithm has a number of places where a quantum gate has two inputs and one of the inputs is known to be classical data. It is often the case that one or more gates can be removed, or that a two-input gate can be replaced by a one-input gate.

Example: Compare a qubit with another qubit bit, fully quantum:



Example: Compare a qubit with a 0 bit, semi-classical:



Note that both kinds of Compare output a quantum value. If the input was k (|0> + |1>), then a compare_with_zero operator will produce a superposition output.

The data comparison (or the logical comparison) is not the same as "Is this superposition state the same as that superposition state?" To do that is more complicated. When doing a full phase comparison, the entanglement value matters.

GPT Revolution: Reimagining Programming in the Era of AI

by kuraz

As we traverse the tech-savvy world of the 21st century, programming is evolving rapidly. The traditional norm of tedious hand-coded scripts and hard-coded solutions is being disrupted by an AI model: ChatGPT developed by OpenAI. This advancement, fueling the transformation, is subtly yet steadily reshaping the programming landscape, bringing monumental changes to the very essence of how humans and machines interact.

ChatGPT, based on OpenAI's GPT-4 architecture, is a language model AI designed to generate human-like text. It can understand context, respond to queries, draft elaborate essays, or even craft a poem. However, its utility is not confined to these tasks. One significant area where GPT-4 has started to show a profound impact is the domain of software programming.

The ChatGPT Wave in Programming

The implications of ChatGPT for programming are vast. It opens a realm of possibilities for developers, enabling them to write code more efficiently, learn new languages or technologies seamlessly, debug errors, and even design architecture.

For starters, ChatGPT can autogenerate code snippets based on descriptions, simplifying coding for beginners and experts alike. Developers can feed the AI a brief on what they want, and the model will generate an appropriate piece of code. This feature makes programming much more inclusive, as even non-programmers can take advantage of this tool to implement simple automation or create basic scripts.

The model also plays a crucial role in learning and debugging. When faced with a new programming language or an unfamiliar technology, developers can turn to ChatGPT for assistance. The model can provide syntax, examples, and descriptions, making learning a new language feel less like translating from an alien script. Debugging is another tedious process where the AI model proves useful. ChatGPT can suggest potential solutions to bugs or even predict where an error might occur, reducing debugging time.

In software design and architecture, ChatGPT's potential is starting to unfold. The model can provide architectural design suggestions, allowing developers to see different potential solutions. Developers can interact with the AI, discuss their needs, and receive instantaneous feedback.

Enhancing Collaborative Coding

ChatGPT's influence extends beyond individual programming; it's changing how we collaborate and share knowledge in the coding world. In a way, the AI model is acting as a team member who's available 24/7. Developers can bounce off ideas with the AI, review code, or receive assistance in understanding a piece of code written by another developer.

In the open-source community, where collaboration is the backbone of projects, ChatGPT could be a game-changer. It can guide developers in understanding complex code, offer suggestions, and help in maintaining the code, thereby making the whole process more efficient.

Ethical Considerations and Challenges

However, this new wave of AI-assisted programming does come with its share of challenges. There are concerns about code plagiarism, where the model might generate code that mirrors copyrighted code. The line between auto-generated code and creativity becomes blurred, raising questions about copyright infringement and intellectual property rights.

Another significant concern is the potential loss of jobs. With AI models capable of writing and debugging code, the fear is real that this might lead to job losses in the software development industry. However, it's crucial to remember that while AI can assist and automate, the creativity, critical thinking, and decision-making abilities inherent in human developers are irreplaceable.

The Road Ahead

Despite the challenges, the benefits that ChatGPT bring to the table cannot be denied. It has the potential to make programming more efficient and inclusive. Programming could become more of a high-level task, focusing on the what and why, rather than the how. Developers can focus more on solving problems, designing software, and providing value, rather than getting bogged down in syntax and code lines.

In conclusion, the advent of ChatGPT in programming is not just about reshaping how code is written; it's about redefining how humans interact with technology. We're moving towards a future where humans and AI collaborate, each leveraging the other's strengths to create better, more efficient, and inclusive solutions.

As we tread this path, it is crucial to balance the unprecedented potential of AI with thoughtful considerations of ethics and inclusivity. In doing so, we can ensure that this technological revolution benefits not just the programming industry, but society at large.

This article has barely scratched the surface of the profound implications and potential of AI-assisted programming. We are only at the dawn of this revolutionary era and, as we delve deeper into the possibilities, one can only imagine how far this AI wave will take us.

Snitched Out by Tech

by Anonymous

Everything is snitching on you these days. You're buying a fancy remote-controlled car, your child accidentally hits old grandma, she hits the curb with her head, and you're getting to jail. Why? You weren't even there. And your little one ran away when he heard siren lights. But this little remote-controlled device has a serial number. They track it down, pull your details from the manufacturer's website, and boom! Your credit card, address, full name. It's all there, waiting forever in the database. It's now you who killed grandma. Good luck fighting this in court!

Imagine you bought a drone, just to make some good number of vacation trip pictures or even videos. It's a new version now and you sold the old one on Facebook Marketplace. This old one goes to Ukraine, or Palestine. Then it ends up in the hands of Mossad, or MI6 - you name it. It has a serial number, they track it down, and you're now a terrorist. They even have an amendment that allows them to charge you with terrorism without too much evidence. Bad luck caused by "good" intent.

Did you know they even put a microchip in sneakers? It's not even visible. A serial number that "protects" against counterfeits. They can track you down, a peaceful protest supporter who accidentally lost one shoe is gonna go to jail. Even if nobody ever gets caught, they can definitely find you and prosecute you for being at a certain location at a certain time.

Clothing? Here is what they say: "starting from the Fall Winter 2020-2021 collection... garments can be authenticated, wherever they were purchased, either by using the 12-digit code or by using a mobile phone to scan the QR Code." Your t-shirt, jacket, shoes, phone, your drone, your remote-controlled toys, headphones, you name it, has a number that can be used to pull all information on you. We're like giant walking trojan horses, paying for things that don't make us free.

Is there a guarantee that your next t-shirt won't have invisible code that can be used to track you down? Some time ago we freaked out how color printers used to print barely visible yellow code so the serial number could be tracked.

Maybe I'm saying obvious things, but it's a new reality now. In this regard, used things are better. Amazon is better than the official website. eBay is better than Amazon. Craigslist is better than eBay. And garage sales are better than Craigslist. Leave no trace. Time for burner emails, burner social media accounts.

You won't get the freedoms that we had before. If even possible, it would take a great deal to get them back.

I Fight for the Users

by The_Gibson

As a member of the Veilid team, Defcon was a wild ride. My full experience was that I arrived on Sunday as my wife was working for The Diana Initiative. As we got to our room and I looked out the window, we had a spectacular view of the Sphere (it is an impressive thing to behold) and Caesar's Forum... and for the rest of the week, I would find myself in a mental battle with the building that would be where we unleash Veilid upon the world. I continued to vacillate between feelings of self-doubt and world domination. How did I end up here? A director of the Veilid Foundation, and some sort of imposter that was getting the childhood dream of working with cDc and bringing hackers.town's unique chemistry of talent and revelry to finally take the first big step to restoring the future. The Rohan to their Gondor....

Those thoughts would steel me over the next five days, knowing what was coming. We had done the legwork, the core development would finish up a mere 48 hours before we went full on Defcon takeover mode, the party was planned, the talks were ready, and The Internet would never be the same again.

This all started back in January of 2020 when I heard the first rumblings about Veilid. Many of you who know me from hackers.town know that I have long been quite vociferous about restoring the future and working to change the world. I still believe in the early promise of the Internet, you know, before we all collectively decided someone else should handle everything, and it all went to shit. At the time hackers.town had some regular meetings going on: a voice chat where we would bounce ideas off one another and think of ways to impact the arc of user privacy and protection. This was largely due to my attendance of Defcon in 2019, and a couple of talks that even further pushed me to want to make big impacts. We had unique talents and reach that had come together in the culture of

an emerging decentralized network, and Bruce Schneier saying "if it's for the public good, why are you waiting for permission?" may have instilled a tiny bit of insanity in me.

Projekt:ONI (Optimistic Nihilists Inc.) was born in this timeframe, and those calls we were having would lead to a regular (almost nightly for a while) cadence for us to start building simple things that anyone could use to ensure their privacy. Dildog had noticed we were having these, and asked me to remind him, and he'd try to drop in someday....

In January, one cold Friday night, Dildog dropped in. The whole room was stunned that our little cargo culting attempt at rekindling the hacker spirit into the world brought someone who did this before into the room. I remember having to help drive the conversation, because I think most in that room were stunned into silence. Dildog proceeded to lay down the idea of exchanging messages in a cryptographically secure manner in which the db was effectively a distributed hash table. We talked for maybe 30 to 45 minutes, and the instant he left the room everyone was trying to grok the wisdom that had just been laid down.... Time would pass, and a pandemic would start.

Our community would end up helping save worlds side by side with other hacker cults over the next few years, helping to build one of the world's largest distributed super computers with r00tfolds, and raising funds to save lives in the early days of the war in Ukraine, even presenting at HOPE 2020.

During the pandemic, I made a trip to Defcon in 2021... against all wisdom. I needed to meet back up with my people. It was a very small year due to the travel difficulties of the time. But risk it we did. Dildog introduced me to Medus4 and TC. It was clear that a team was starting to form, and the project actually started to take shape, and for the first time I could finally start to make out a path toward a future restored. We brought together a team of volunteers and got to work.

We were going to do this and dent the universe.

Fast forward a few years: August of 2023. Veilid had been operational for a few months, and revisions and updates to get to somewhere between an alpha and beta state finally got finished just days before the Friday launch. The party was planned, the team was onsite, and the hot dogs were in Veggie's possession. Only now were we beginning to understand the level of excitement around this launch. I had run a fundraiser a few months before, selling Veilid t-shirts to get money to fund this crazy excursion... and they were everywhere. It's always surreal to see people you don't know wearing the markings of your thing... but this was at a whole new level. Our little social media blitz had delivered.

What Is Veilid, You Ask?

The intent of the Veilid project and Veilid Foundation Inc. is to create a privacy centric network that enhances human privacy in communications. We believe that the Internet has yet to fulfill the future role once promised and, as such, we refer to this new operating model as Web 1.5. We want to enable people and developers to break free of the data silos that have so long monetized our information. Personally, I see no separation between the data constructs that people generate in their communications and their physical person; they are both a part of you, so the idea that we can sign part of ourselves away via an end-user license agreement (EULA) is, at its core, problematic. Ultimately, we wanted a better option to support restoring the future we were promised when the web was young, and as such we consider this Web 1.5... what should have been.

Veilid is an application framework designed to allow developers to be privacy first. Veilid is also a routing protocol that enhances the privacy of the users of the network. It uses distributed hash tables for storage. It is conceptually like IPFS plus Tor, but faster and designed from the ground-up to provide all services over a privately routed network. It enables development of fully-distributed applications without a "blockchain" or a "transactional layer" at their base.

Veilid can be included as part of user-facing applications or run as a "headless node" for power users who wish to help build the network.

In 1999, cDc showed up and asked you to show some control when they launched Back Orifice 2K.... Now we are telling you all to take back control.

You want to help take back the wires, and enshrine privacy as a human right?

Go to `veilid.com/contribute/` and see if there is any way you can pitch in.

We Need:

- coders and hackers
- app developers
- usability experts
- translators
- open source governance
- donations

Together, we can build a better, more private Internet. Join us and help us restore the future!

ARTIFICIAL INTERRUPTION

by Alexander Urbelis

On Trust and Moral Clarity in War Time

alex@urbel.is

I was in Israel nearly ten months earlier to the day of penning this column. Listeners of *Off The Hook* may even recall that I appeared on the radio show from Tel Aviv and was raving about the place. It was my first time in Israel and I count myself lucky to have been there before hostilities erupted. I found it to be a very special place, holy in its own right for several reasons, but special in ways that had nothing to do with it being the birthplace of most major religions. Tel Aviv was bustling with life, the food was delectable, the architecture was unique and gorgeous, the people were welcoming, Arabs and Jews played football and ate together in Jaffa, and I learned that Tel Aviv was one of the most accepting places for the LGBTQ population in the globe, let alone the Middle East. The juxtaposition of earnest modernity with orthodox Judaism, however, can lead to some strange experiences, a perfect example of which happened to me in a taxi on the way to a meeting with clients.

It was midday in Tel Aviv, and I had to get from the city center to Herzliya in the north to meet clients and present on legal issues relating to AI developments. A colleague and I hailed a cab. Making some last-minute tweaks to the presentation while en route, I had my laptop open and did not pay much attention to my surroundings. I did notice that the driver appeared to be a serious-looking, religious, orthodox Jew. A few minutes into the journey, my colleague and I looked at each other quizzically and in some disbelief at the sounds emanating from the back seat speakers: a woman moaning, not in distress, but in what appeared to be ecstasy that was continually growing in cadence and decibels, culminating in what was almost certainly an orgasmic climax, with a musical accompaniment and periodic interruptions of a deep-voiced Frenchman.

I recognized the moaning. It was the Serge Gainsbourg song, "Je t'aime... moi non plus," or, in English, "I love you... me neither." Released in 1969, the song became an international hit, but was banned in several countries, including the United Kingdom, Italy, Spain, Sweden, Brazil, and was forbidden from being played on the radio earlier than 11 pm in France. Radio stations in the United States were not prohibited from playing the song, but they barely did, deeming the orgasm sounds of the end of the tune a bit too risky for their taste, even in the 60s and 70s. The Vatican denounced the song and, according to some accounts, even excommunicated an Italian record executive who was involved with the song's release in Italy. Attributing the song's success to its taboo status, Gainsbourg was quoted as having said that the Pope was his best PR man. Despite this ban spanning Europe, Scandinavia, and South America, and the ecclesiastical condemnation of the same, our overtly religious driver seemed entirely unbothered by any aspect of this historically scandalous song.

Such censorship across geographies is a thing of the past - we would not bat an eye at the sounds of orgasmic ecstasy on our radio waves these days - but required a certain type of moral clarity that also seems to be a thing of the past.

It's no great revelation that we are barraged with information. That's been the case since the commercialization of the Internet. But since that time, the signal to noise ratio has been skewed more and more in favor of noise rather than signal. Today, with two wars waging simultaneously - Russia v. Ukraine and Israel v. Hamas - there is a pressing need for the sort of moral clarity that they had in the 60s.

Again, listeners of *Off The Hook* will recall that we recently had Dr. Welton Chang, CEO of Pyrra Technologies on the show. Pyrra is a company that monitors alternative social media outlets, such as Gab, 4Chan, Truth Social, and other far-right and extremist platforms. Dr. Chang opined that the extraordinary amount of high-definition wartime video footage that is available to anyone today is unprecedented. Bad actors spreading disinformation have at their fingertips a great many choices of violence and gore that can be re-purposed for whatever deceitful purpose.

Along similar lines, nearly two weeks after Hamas attacked Israel, Michelle Goldberg penned an op-ed in *The New York Times* entitled, "It Is Impossible to Know What to Believe in this Hideous War." The starting point for that article was Goldberg's lamentation of the fact that she did not know what to believe concerning whether the rocket that destroyed a hospital in Gaza was of Palestinian or Israeli origin. Many people are likely still confused by this, and still

others will almost certainly dismiss the factual findings of the U.S. intelligence community that Hamas forces were responsible for the firing of that dreadful rocket. The reason being it's far too easy to find whatever disinformation supports the reality you prefer in the digital cacophony in which we find ourselves.

This disaster, however, is exactly what social media platforms want. No matter the type of investigation, it is always important to ask the question of *cui bono,* or who benefits? With Twitter/X, the removal of the content restriction guardrails around mis/disinformation - under the pretense of the promotion of free speech - has a net effect of benefiting the platform itself. While this may be short-lived, with advertisers leaving in droves and several failed initiatives (think of the blue check fiasco, et alia), any burst of platform activities may reassure investors and drive additional advertising revenue to a platform.

Why is it that we are drawn to this fray in much the same way that we are drawn to elements like the Serge Gainsbourg song that pique our prurient interests? Perhaps the answer has to do with evolutionary biology.

We are drawn to conflict. We like to fight. We like to watch fights. And when platforms allow us to be spectators to throw-down quarrels, all of which are based on speculative and questionable information, platforms are exploiting our basest pugilistic and atavistic instincts to drive, and keep, eyeballs on their systems so that they can collect more data, analyze our behaviors, derive yet even more data, and then sell that data to third parties or use it to obtain additional advertising dollars.

If we think back to the Arab Spring about 13 years ago, social media played a significant role in organizing and disseminating information from the front lines, an inspiring role no doubt that ignited much of North Africa and led to the toppling of several dictatorships. But the weaponization of information at a scale then unimaginable has severely outstripped platforms' ability to create, let alone enforce, reasonable policies to stem the flood of disinformation or even blatantly false information. Yet, these platforms want us to trust them and rely on them more than any mainstream media. According to the platforms, the mainstream media are leftover dinosaurs gasping for air wandering around the Chicxulub crater and wondering what all the dust is about.

But there is a reason why the so-called mainstream media has persisted for centuries, why the *Oxford Gazette* has existed since 1665 and *The New York Times* since 1851: because they have held true to their ethical obligation to fact-check information before publication and have earned, not demanded, the trust of their readers. The reason why the founding fathers of the United States enshrined the freedom of the press as part of the First Amendment to the Constitution is because they recognized the critical role that having an informed populace plays in maintaining a democracy.

If we are to have a government of the people, by the people, and for the people, then all people need to be able to assess and make moral judgments about the behavior of the government, its officials, and have at least some rudimentary understanding of global affairs. But how can we expect there be moral clarity without factual certainty?

We cannot. What the Israel-Hamas and Ukraine-Russia wars are making quite clear to us is that social media platforms are ill-suited tools to assist with factual and moral determinations. Platforms are ill-suited for all but the most casual and inconsequential dialogue or exchanges. Social media should not be used for news gathering, political discourse, or dialogue between nuclear powers. Yet, time and again, because of the attention the platforms shower on the speakers - regardless of truth, accuracy, ethics, which in turn provides an incentive to a speaker to be as incendiary as possible to amass a greater following - it is exactly where all of this occurs.

The other battle that has been raging quietly for some time now is for our attention, our time, and our data. Akin to rising popularity in the 70s of Serge Gainsbourg's works banned for obscenity, we stay drawn to social media not because it fosters any sense of meaningful community, but because of our prurient, salacious, and voyeuristic interests - in much the same way that supermarket tabloids flourished in the 1990s. We should learn from the veritable horror show that Twitter/X has become that there is nothing to be gained from engaging; if we disengage, so shall others, and when a majority disengages, social media will lose its ability to influence world events and its ability to sustain itself.

I submit that it's time to pull the plug, to reclaim the power of moral suasion that social media has usurped, and to the degree possible we should revert to traditional and trusted sources of information that have served us all well our whole lives. Marshall McLuhan once said of newspapers that, "People don't actually read newspapers, they step into them every morning like a hot bath." And, after reading the paper, or this article, if you want to turn on the radio, I can recommend a good station that broadcasts from Tel Aviv.

Platform Capitalism
Can't Surveil Absurdism (and Worse)

by Nicholas Croce

Olive DM'd me on Twitter in May 2022: "Boy have I got a story for you." It was an odd message, out of the blue, from someone I didn't know. As a researcher of technology and capitalism, I had been studying NFTs "on scene" for about a year, traipsing between some of the bizarre online chatrooms in which electronic assets are hyped. Taking a quick peek at Olive's profile, I saw Milady Maker art everywhere, collaged/edited/memed, along with the absurd style of posting they call "network spirituality." I knew about Milady because their NFT art stands out so much: the art is bizarre, the tweets quirky. If the average Internet user stumbled across one of these tweets, they'd think little of it besides, "that's weird." Seen in context or community, though, the social performance is *political*.

Me and Olive have at least one thing in common: On a place like the Internet where everything feels copy-paste, some of us are looking for something else.

So I took the call with Olive. They led me through their story, from that late night in August 2021 with Prelon, to their ghosting of the Second Milady Rave due to "vibes," opting for a night at home with some NYC artists-turned-Milady folks and a "big bag of ketamine."

Olive had a lot to say and gave me a crash course on, well... I'm not completely sure. They explained that finding "avant NFTs" on the stale NYC art scene wasn't about crypto, at least not at first. For them and some other underground NYC artists, it's something bigger, something called "network spirituality," a way to use the Internet that rejects just about everything your parents might accept about the Internet. First and foremost, this spirituality is "post-authorship," where everything is a meme, i.e., graphic and textual art is made for repurposing, à la Barbara Kruger and collage, but rapidly, on the network, no citations and no credit. As Olive put it, "Symbolic signifiers... network spirituality... once fluent, you can feel the network. People have the capacity to develop a sense. It's a spiritual process where the self is sublimated into the network." According to Olive, some (including an Internet artist and activist named Charlie) conjure something called a "tulpa," a being that inhabits the body and can then perform on the network. The tulpa is just one of many occult and esoteric references being used by practitioners of this odd way of using web platforms.

Let me back up. Before I tell you Olive's story - typical of a way of exploring the Internet which I think is becoming increasingly common - here's some context.

There are two narratives about the Internet. The most common one circa 2023 looks something like this. In the beginning, the Internet was a disparate and purpose-built place. Niche segments of society - academics sharing scientific data, the military communicating battlefield maneuvers - used and developed the Internet. As the Internet became commercialized, an eclectic assortment of online services arose to, first, meet specialized and business needs, and later, those of the general public. Fast forward: the dot-com bubble bursts, hastening the consolidation of the Internet into a succession of platforms. Before there was Facebook there was Myspace, and before that there was AIM and AOL, and before that GeoCities, and on. Now, what happens on the Internet occurs thanks to an increasingly concentrated number of service providers. In this view, the Internet is a useful place that is free to use, has more than enough to offer, and is loved by your parents.

There is another story of today's Internet, and it's probably not one you know. The Internet was developed as part of the U.S. government's command and control structure in the thick of the Cold War. Since then, the Internet has coalesced into a growing number of platforms operated by a shrinking number of tech giants - and tech oligarch-bros. In this narrative, there's a small cadre of Internet users who are fed up with it all, especially social media. They look for and use alternate platforms. Sometimes they build their own. These users are uncomfortable with Internet companies like Meta - Facebook's parent company (and Instagram's, and WhatsApps's) - owning, analyzing, and ultimately adapting their services in real-time to increase screen time, monetizing each click and

view. Hence, the Internet is a web of contested spaces under strict and constant surveillance - and is best enjoyed when highly memeified.

Olive's story asks an important question: What happens when artists, anarchists, and increasingly, just random people making memes on the Internet, do things that aren't anticipated by today's Internet platforms?

Late one night in August 2021, Olive was scrolling, and looking for something. Outside, the latest COVID-19 surge was ripping through New York City. Olive, a NYC-based artist, had just moved into a new apartment in Brooklyn. Despite their wealth of connections in the city's art world, they felt a lack. They were bored. And like so many of us, they started scrolling.

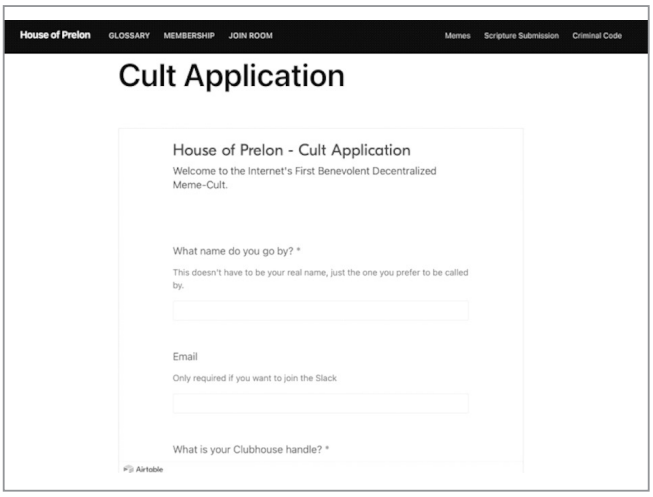
"I was in love. It was the feeling of being in love. I hadn't spoken to anyone intimately. It was the pandemic. My brain was on fire."

Olive was attending an event on Clubhouse, an invite-only Internet space popular for its long-form voice chats. Olive was frequenting science and policy voice chats hosted on the platform. As one event wrapped up, an unruly attendee shouted, "Clubhouse was better before Elon!" The platform suddenly resounded with shouts of "Prelon! Prelon!" In a space full of Internet elites and self-billed intellectuals like Clubhouse, this wasn't supposed to happen. But, as it goes with so much of Internet culture today, people began organizing themselves ad hoc. A new chatroom was born. Those participating in this impromptu community donned profile pictures of Elon in garb resembling that of Jesus. A meme was born, too.

So what?

Love, if you ask Olive. The chatroom, named "House of Elon", became a calm albeit absurd space. They loved everything about it. "Welcome, Olive" the profile pictures of each Prelon acolyte would soothingly call out when Olive entered the room. In a time of pandemic, the House of Elon was e-stability. Members talked politics and current events. They posted obscure memes. Linking to other online spaces of interest was common. Olive recalls fondly that everyone took turns.

One response to a centralizing Internet is the construction of fringe, elite spaces, and that's exactly what's happening across the Internet today. And, if you go on the House of Elon's website, you can even join... via a "Cult Application." A meme was iterated.



As memes iterate and circulate through chatrooms on the Internet, so do users. Olive met another user, Charlie, in a Discord chatroom (a "server") called Wet Brain Podcast. It had come highly recommended by fellow Prelon prelates. "Hey, I'm doing an NFT project," Olive recalls Charlie messaging the server. Thinking back, says Olive, "I'm thinking, whatever... we're all artists, and I didn't know really know what an NFT was... and $300? I couldn't fathom it."

That quickly changed.

To some, Charlotte "Charlie" Fang is a cult leader.

Lots of people from the New York art scene were in the Wet Brain Podcast server. Certainly, some, like Olive, had made their way there from the Prelon chatroom on Discord, but they came trickling in from chatrooms and social platforms across the Internet. Many users were young and making art. All of them were looking for the next big thing. "There's nothing avant garde about the gallery scene in New York. 1980 to 2022, there's no difference, no new language, the so-called avant garde artists today are just using different images." So, with curiosity and extremely limited knowledge of what an NFT was, Olive clicked on Charlie's link. They were blown away. This was what they had been looking for: something fresh, not rehashed collage work, not tired ideas. The NFT project was called Milady Maker, created by a pseudonymous Internet collective called Remilia. At first, Olive bought just one, spending about $300.

The NFTs were hugely unpopular and sales

stagnant. Olive, though, was hooked: on the ideas and art of these niche spaces, on going from niche to nicher Internet space, on Charlie. They were electronically following Charlie's work and those attracted to it, hopping from chatroom to chatroom, unbound by any social platform. What Olive saw from Charlie impressed them immensely. Charlie was building their art brand in niche sections of the Internet. Hell, Charlie co-founded a decentralized autonomous organization (DAO), a kind of Internet collective that uses cryptocurrencies to pool funds and make investments. The DAO, called SpiceDAO, had purchased an illustrated manuscript of *Dune* at auction using $3 million in crowdsourced funds, with plans to license its artwork and redistribute the proceeds. The art and hustle of Charlie elicited interest from starving artists like Olive who wanted something else out of art - and life generally. This electronic art was being circulated in multiple, niche yet global Internet spaces, and all kinds of users, including many NYC-based artists, began to latch onto Milady Maker.

Around February 2022, things began to look up for Milady Maker, Charlie, and the Remilia Collective. Anonymous individuals associated with the Collective (some met pseudonymously online, some knew each other from the New York art scene) planned a so-called "Second Milady Rave" in a speakeasy in Manhattan's Little Italy. As Olive tells it, the party was quickly scuttled by the police. Public records confirm that a party was broken up in early March 2022 for underage drinking. Regardless of the actual event, the spectacle of the Second Rave, as memorialized by memes, was pivotal for the NFT's success. What started (at least on its face) as a niche social media phenomenon was hot on NYC's underground (and young) art scene. In the weeks that followed the Lower Manhattan bust, Milady Maker NFT owners used (i.e., posted, iterated) memes and used guerilla art tactics to advertise their NFTs and their community. The project quickly sold out, delivering about $3,000,000 in proceeds to Charlie and those associated with Remilia. Olive, who by now had purchased six Milady Maker NFTs for just under $2,000, saw the value of their collection grow to well over $10,000.

The "big story" Olive mentioned to me wasn't about Remilia's success. What Olive really wanted to tell me is that something had shook the Milady world, including many in their "in real life" circles. Charlie, the pseudonymous Internet figure at the head of Remilia, had just stepped down. There were tremendously concerning allegations being made against Charlie by other practitioners of network spirituality, a wide variety of accusations: like that Charlie had been pivotal in growing a white supremacist cult on the website 4Chan, and that accounts used by Charlie had groomed and abused young women drawn to their art. Charlie had even taken to Twitter and admitted to parts of it. Documents reviewed show disturbing, misogynistic, and abusive behavior by pseudonyms associated with and adjacent to Charlie. One image, a poster entitled "Sonya's Rules," is pink and features a picture of Hello Kitty; its content is highly misogynistic and seems meant for grooming young women.

A few days after my call with Olive, I received another call, from a number I didn't recognize. Y, who remains anonymous, said, "I heard you were writing a story about Milady. I was groomed." Y, who lives in the United States, had been paid to moderate a chatroom and relay information about the people who found their way there. About their role, Y said, "My job was to talk to them, girls, entertain them, and report back with screenshots of the conversations I was having. Sonya would say, 'Good job, Y. Good conversation.'"

I asked Y what happened next: "I don't know, and I didn't care."

The identity of Sonya remains unclear and will likely remain so. Olive says it's a pseudonym used by Charlie while others disagree and say Sonya was an early art collaborator with Charlie and their pre-Remilia collaborator, Sunny. One user, C, a blogger and Internet artist, is concerned: "I genuinely believe a lot of the stuff is real and the 'art project' is a flimsy excuse that is doing a good job of tricking a ton of people."

When everyone is using pseudonyms, making niche and sometimes offensive art, and doing network spirituality, it's hard to tell exactly what's going on.

Charlie stepped down around the time Olive called me. They had admitted to Miya, a pseudonym associated with one of the "art

projects" C referred to. Miya's Twitter account has been suspended. I reviewed an archive of Miya tweets as part of reporting this story. They are chock full of racist and far-right ideas. Charlie, though, offered an explanation.

As I was writing this story, I received a notification of a Twitter Spaces, an impromptu and public voice chat - with Charlie in it. So, I jumped in, into a birthday party thrown for Charlie by the Remilia Collective, from which Charlie had stepped down a few weeks prior. Charlie explained Miya like this, "It was a project... [meant for the] acceleration of ideologies embedded in 4Chan and obscure hobby communities to absurdity, to the absurd limits. It combined Landian acceleration, post-humanism theory fiction, and performative posting... Miya engaged in accelerationist philosophies... performative literature. I believe in cyber anarchism and free speech."

Olive, who manages a New York City art gallery and is an artist in their own right, went from a bored pandemic night looking for good art to cyber anarchism.

***

To what extent had I, the researcher, become a meme?

In a way I think related with this political moment's "post truth," in writing this essay I found it consistently difficult to distinguish fact from fiction. Did Charlie create a cult and groom young admirers? Or was "the cancel" of Charlie only a meme, and my research had become an iteration, I as the purveyor of a quasi-empirical copypasta? How did Y get my number, and was their story legit? Who the heck is Charlie anyways? And does Olive honestly believe Charlie created a "tulpa" that was "born in their gut?" This confusion is consequent of the cyber anarchist approach to intervening against an Internet these users loathe. Here's what I think is going on.

In one light, people engaging in avant garde e-art and absurdist "network spirituality" Twitter are this generation's cyber punks. They are young, makers, and rejecting the status quo. Some of them are influenced by anarchist and libertarian ideologies. A few, drawn into the network spirituality practice, in reality hold far-right ideologies and, when confronted with the products of ideological accelerationism as described by Charlie, don't realize that they're being made a fool. Many, many others are simply there for the art, or even more benignly, simply there to do something interesting and be a part of something, like make and share memes.

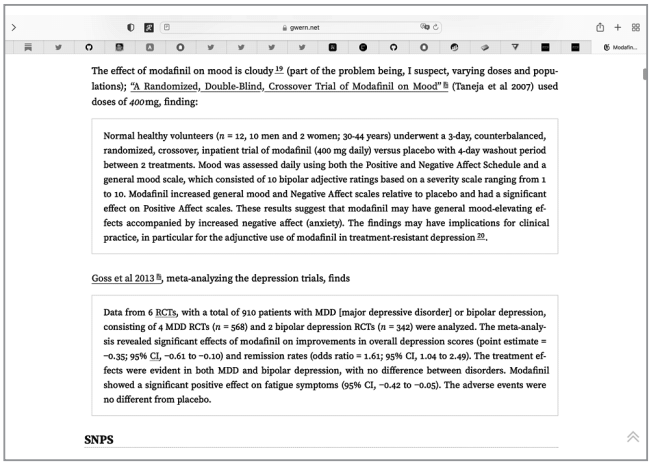
Those who philosophize on network spirituality see the electronic capitalist platforms of the Internet as horrors, and their actions are intended to intervene. As Olive described, "There's the Empire where everything is surveilled. It's full of self-censoring, and it's a dead space for creativity. Think Netflix or Facebook. Then there's the Dark Forest. You can't Google it. You have to find them, these vibrant, self-contained communities. There's no 'trade relationship' with the Empire because the Empire's surveillance is so potent and can corrupt the Dark Forest."

Recall that Olive found themselves in this space by jumping across platforms and spaces: from an elite, invite-only space on Clubhouse, to a reactionary and at first spontaneous (and then fastidiously curated) meme chatroom on Clubhouse, to a Discord room full of NYC and international artists, and finally to Twitter. The forms of posting (iterative, post-authorship, meme) and content of posting (often esoterica) permeate out through the Empire in a process that is enjoyable, creative, communal - and interferes with platform surveillance.

Surveillance algorithms are not programmed for absurdity.

Posting on the Internet against surveillance can have ramifications beyond an intervention against surveillance in and of itself - it can be used to hide illegal activity. A few of the materials I reviewed were ostensibly this, but it's hard to see. For instance, I was sent a website by Olive that looks, at first glance, like a professional homespun website with headlines like "Me" and "News." Searching around the website, I find a lot of things that are bizarre: an in-depth description of the website owner's desk, methods by which their computer was created, the age of their desk chair. On another page, I find an article that promises a "cost-benefit-informed perspective" for a pharmaceutical. It's written like an academic article, with citations, charts, formulas. But it's utter bullshit, and while it's art and perhaps doing the work of philosophical accelerationism in one sense, it's meant to be a hidden-in-plain-

sight linkage into the dark web, one section of the Hidden Forest Olive described. The academic lingo and presentation is meant to fool *both* algorithmic and human eyes into thinking this page is an academic article, as opposed to a linkage to suppliers of illicit drugs and the darknet markets that sell them.



The effect of modafinil on mood is cloudy [19] (part of the problem being, I suspect, varying doses and populations); "A Randomized, Double-Blind, Crossover Trial of Modafinil on Mood" [8] (Taneja et al 2007) used doses of 400mg, finding:

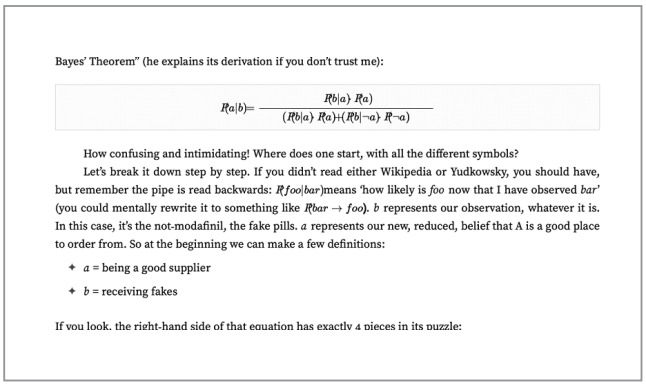
> Normal healthy volunteers (n = 12, 10 men and 2 women; 30-44 years) underwent a 3-day, counterbalanced, randomized, crossover, inpatient trial of modafinil (400 mg daily) versus placebo with 4-day washout period between 2 treatments. Mood was assessed daily using both the Positive and Negative Affect Schedule and a general mood scale, which consisted of 10 bipolar adjective ratings based on a severity scale ranging from 1 to 10. Modafinil increased general mood and Negative Affect scales relative to placebo and had a significant effect on Positive Affect scales. These results suggest that modafinil may have general mood-elevating effects accompanied by increased negative affect (anxiety). The findings may have implications for clinical practice, in particular for the adjunctive use of modafinil in treatment-resistant depression [20].

Goss et al 2013 [8], meta-analyzing the depression trials, finds

> Data from 6 RCTs, with a total of 910 patients with MDD [major depressive disorder] or bipolar depression, consisting of 4 MDD RCTs (n = 568) and 2 bipolar depression RCTs (n = 342) were analyzed. The meta-analysis revealed significant effects of modafinil on improvements in overall depression scores (point estimate = −0.35; 95% CI, −0.61 to −0.10) and remission rates (odds ratio = 1.61; 95% CI, 1.04 to 2.49). The treatment effects were evident in both MDD and bipolar depression, with no difference between disorders. Modafinil showed a significant positive effect on fatigue symptoms (95% CI, −0.42 to −0.05). The adverse events were no different from placebo.

SNPS

Looks like an academic literature review.



Bayes' Theorem" (he explains its derivation if you don't trust me):

$$P(a|b) = \frac{P(b|a)\ P(a)}{(P(b|a)\ P(a) + (P(b|\neg a)\ P(\neg a)}$$

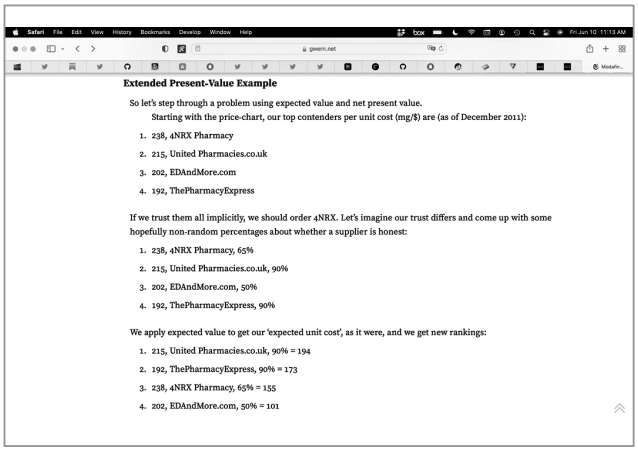
How confusing and intimidating! Where does one start, with all the different symbols?

Let's break it down step by step. If you didn't read either Wikipedia or Yudkowsky, you should have, but remember the pipe is read backwards: $P(foo|bar)$means 'how likely is *foo* now that I have observed *bar*' (you could mentally rewrite it to something like $P(bar \rightarrow foo)$. b represents our observation, whatever it is. In this case, it's the not-modafinil, the fake pills. a represents our new, reduced, belief that A is a good place to order from. So at the beginning we can make a few definitions:

- a = being a good supplier
- b = receiving fakes

If you look, the right-hand side of that equation has exactly 4 pieces in its puzzle:

If you scroll down, and down, and down some more, there's silly formulas that don't mean much.



Extended Present-Value Example

So let's step through a problem using expected value and net present value.

Starting with the price-chart, our top contenders per unit cost (mg/$) are (as of December 2011):

1. 238, 4NRX Pharmacy
2. 215, United Pharmacies.co.uk
3. 202, EDAndMore.com
4. 192, ThePharmacyExpress

If we trust them all implicitly, we should order 4NRX. Let's imagine our trust differs and come up with some hopefully non-random percentages about whether a supplier is honest:

1. 238, 4NRX Pharmacy, 65%
2. 215, United Pharmacies.co.uk, 90%
3. 202, EDAndMore.com, 50%
4. 192, ThePharmacyExpress, 90%

We apply expected value to get our 'expected unit cost', as it were, and we get new rankings:

1. 215, United Pharmacies.co.uk, 90% = 194
2. 192, ThePharmacyExpress, 90% = 173
3. 238, 4NRX Pharmacy, 65% = 155
4. 202, EDAndMore.com, 50% = 101

Finally, we get to the websites where we can order modafinil, a controlled substance. The text is written to look like an academic analysis, but it's nonsense. Out of the way of the prying e-eyes of surveillance and the uninitiated, for those who know where to look, it's likely there's a lot more here.

Did Charlie's anti-surveillance radicalism create a shelter for others, like Sonya, who weren't there to make a political statement but to exploit a weakness of platform governability, using the chaos and "performative literature" of Internet spirituality as a cover? This type of writing against Internet platforms obscures reality from both human and electronic eyes. In terms of platform surveillance, algorithms aren't equipped for the depth of meaning laden onto meme images and memetic writing., And when it comes to users, the problem of collectively governing an Internet space is just as formidable. Most practitioners of Internet spirituality I've spoken to in the year since the allegations of misconduct were first made state strongly that the grooming didn't actually happen. I asked one user, "Are you sure you knew what was real and what wasn't?" They responded that they in fact did, since some of the most widespread allegations had been "copypasta," a type of text-based meme. My reply?

"Have you considered that bad actors from within or outside of the community could subvert a meme for their own purposes? Isn't that foundational to a meme in a way?"

Charlie, during his birthday party, stated forcefully that Remilia and network spiritualists "reject ugliness." How can we know? During Charlie's birthday party, which was attended by many NYC artists, some railed against "cancel culture." Charlie said, "Cancel culture is a huge problem in art." Unfortunately, what I think this thinking tends to enact in these spaces - and increasingly on the Internet as a whole - is a rejection of *accountability* culture. Charlie claimed that, "the Internet itself is anarchist" and I can't disagree more - the Internet is programmed. In real life, we have people, we have norms, and we have spaces. People can come together, co-construct a specific space, and establish norms for that space. We all know how to "program" a physical space because we're social creatures in an embodied world. Internet culture will always have built-in nihilism until we devolve the tools of building the Internet into the hands of everyday users - we're all either using big tech's platform or no

one's in particular. Meanwhile, memes seem to have a tendency to move the real to the spectacular, and to talk about the real using the spectacular has ramifications.

Society at large can't program our Internet spaces. But it must if we're going to live there.

Can network spirituality defeat the surveillance systems that are necessary for social media sites like Facebook and Twitter to work? As someone who studies platforms, I think the answer is yes, at least for the battle between today's machine learning algorithms and today's network spirituality absurdism.

After my conversation with Olive, I can't help but think that so much of Internet culture has taken on cult-like appearances. We share memes and GIFs to show our understanding of increasingly niche cultural knowledges. Spaces on social media platforms are as segmented as ever. The chatroom Y moderated was on an obscure platform most people have never heard of, but is popular for its weak regulation (a fact, perhaps, unknown to many of those who wound up there). As a society we increasingly struggle to tell what's real, and perhaps you've even found yourself saying, "well, it doesn't even matter." Meanwhile, our daily technologies are cybernetic, push notifications timed not to inform, but to make us act, to make us make someone else's value, page refreshing not to connect with others but to see how many likes we've accumulated. The network spirituality of Milady Maker, whether an Internet cult or not, is like so many other absurdist art movements in that its absurdity isn't nonsense, it's a critique. Whether we can co-construct an Internet that is socially governable, with rules made and commonly accepted by its users, seems an open and contested question. How policymakers who want to secure the Internet but keep it free respond to this critique remains to be seen.

Alzheimer's and AR Tech

by Mx. Blu3

Augmented reality could help people with Alzheimer's or early dementia find their way home, as well as with running errands like shopping or buying groceries. Just as smart devices already monitor people's health (like the Oura ring) and devices like Apple and Samsung tags already help us locate our keys or our cars, Alzheimer's patients could utilize the same form of technology to help with living their lives with dignity and independence. This would also potentially be a much more cost-effective option to hospice or live-in care, which is expensive, and the costs for such care have been increasing.

Not all older phones support augmented reality, but the technology, which includes both software and wearable smart devices, is already here now, albeit a bit pricey. Both the iPhone and Android platforms include augmented reality apps that enable outdoor and indoor navigation using AR technology for directions.

The most important thing would be making sure that people with Alzheimer's have these devices on them at all times, *and* that they're aware that they have the ability to use them and not be ashamed to. One way might be preparing people who may be experiencing onset symptoms to habitually start using such software paired with a smartwatch and smartglasses combination so that it becomes second nature to finding their way home when it comes to getting lost. You could also set the home address ahead of time, so that simply saying "take me home," "home," or "need to go home" enables the feature. However, it works the other way around too; AR could also allow bystanders to assist people with Alzheimer's who are lost in getting home. Plus, smart devices will only go down in cost making them more accessible to the older community, making this an available cost-affordable option for those on a fixed income with retirement, but policy makers could have insurance cover this for health purposes in the future.

This is important because physical activity and exercise are also important when it comes to the early to middle stages of dementia and this would not only give people with Alzheimer's the ability but also the independence they need to perform such activities themselves. Hospice care for people with dementia has become very expensive and not everyone will be able to afford such care, or to be able to be placed in an Alzheimer's village, something that other countries such as the Netherlands are starting to implement. Technology is meant to make people's lives easier. Augmented reality paired with smart technology may present a possible cost-effective option.

Book Review

***Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity and Democracy,* Laurent Richard and Sandrine Rigaud, Henry Holt and Co., 2023. ISBN 978-1250858696**

Reviewed by paulml

This is the true story of the newest way for governments to spy on their citizens: through their cellphones. Using a vulnerability in iPhones, an Israeli company developed a way to install malware on a phone. It would allow the government to upload the phone's entire contents (photos, phone numbers, and text messages) without the owner's knowledge. It was marketed as a weapon against terrorists and drug dealers. For authoritarian governments, like Morocco and Azerbaijan, journalists and dissidents belong in the same category as terrorists.

A group of French investigative journalists received a leak of 50,000 phone numbers from Pegasus, grouped by country. The first job was to match a number to a specific person, without the person knowing. The hardest part was to ask a journalist in Mexico or Turkey, for instance, to hand over their phone without giving them the reason. It became possible to find Pegasus on a phone. Of the phones that were tested - about 100 of them - the vast majority were infected with Pegasus.

It became necessary to bring in local journalists from all over the world to have them work on local angles to the overall story. Absolute security was essential. The slightest leak could kill the whole project, and cause governments to crack down on their citizens extra hard.

This is an incredible piece of journalism, and it would make an excellent movie. As if anyone needs another reason to fear government surveillance. It is very highly recommended for everyone, dissidents and regular citizens.

Book Review

***Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks;* Scott J. Shapiro; Farrar, Straus and Giroux; 2023; ISBN 978-0374601171**

Reviewed by SEGGY

Fancy Bear Goes Phishing is a very good book by Scott J. Shapiro; fans of *2600 Magazine* should consider reading it from cover to cover.

At the outset, in the introduction, the author avers he has learned "much of what is said about hacking is either wrong, misleading, or exaggerated." Some quoted in the book commend hackers for their skills and ingenuity. His inquiry as to why "the Internet is so vulnerable to attack" shows that the five major hacks recounted benefited from a heedless disregard for needed security in transactions with hardware, software, networks, and humans. Backdoor functions left in the released version of SENDMAIL, one of four attack vectors exploited by Robert Morris' worm which crippled the Internet in 1988, return nearly a decade later in the late 1990s, with power easier to exploit via MS Office macros, also lacking security measures. His telling of Microsoft's delinquent decision - made only after hasty bloatware pushing secured their OS dominance - to prioritize security may be unduly moderate. However, his botnet war accounts astound.

Some hack narratives deserve further technical detail and explanation, but he intelligently situates hacking from wider perspectives of philosophy, psychology, heuristics, citizenship, war, sovereignty, legality, morality, and the limits of solutionism: the idea that technology can solve all problems. He smartly curates an array of luminaries and rogues, from Marx, Trotsky, Snowden, Turing, *Mr. Robot, WarGames,* the GRU, NSA, FBI, Amartya Sen, to Rousseau.

Hacker profiles are scrupulous, filling the book with richly human and technically savvy characters, many who would have benefited tremendously from this book had it been available when they needed a broader outlook on the world in which they were inflicting much havoc.

Those unmoved by the book, the perennial skeptics, are addressed adeptly in the epilogue, so be sure not to miss a single page.

PDF & EBOOK SUBSCRIPTIONS!

Yes, we finally did it! You can now get a PDF subscription or have issues in EPUB3 format for Kindles and other ebook readers. No DRM or any sort of copy restriction! Subscriptions range from one year to lifetime in the format of your choice.

Just visit the SUBSCRIPTION section at 2600.store

PLEASE HELP US SPREAD THE WORD

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** 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.

January 12-14
ShmooCon 2024
Washington Hilton Hotel
Washington DC
www.shmoocon.org

February 17-18
Vintage Computer Festival SoCal
Hotel Fera Anaheim
Orange, California
vcfsocal.com

April 5-7
Vintage Computer Festival East
Infoage Science and History Museums
Wall, New Jersey
vcfed.org

May 4-5
CoCoFEST!
Holiday Inn & Suites Chicago-Carol Stream
Carol Stream, Illinois
www.glensideccc.com/cocofest/

May 17-19
CackalackyCon
DoubleTree at Research Triangle Park
Durham, North Carolina
cackalackycon.org

May 17-19
NolaCon
Hyatt Centric
New Orleans, Louisiana
nolacon.com

June 14-16
Vintage Computer Festival Southwest
Davidson-Gundy Alumni Center, UT Dallas
Richardson, Texas
www.vcfsw.org

July 12-14
HOPE XV
St. John's University
Queens, New York
hope.net

July 17-24
BornHack 2024
Funen, Denmark
bornhack.dk

August 8-11
DEF CON 32
Caesars Forum, Harrah's, Linq, Flamingo
Las Vegas, Nevada
www.defcon.org

August 16-18
Fri3d Camp
Hopper Youth Residence De Kluis
Sint-Joris-Weert, Belgium
fri3d.be

September 7-8
Blue Team Con 2024
Fairmont Chicago
Chicago, Illinois
blueteamcon.com

September 26-27
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.com

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

Events

HOPE XV. The 15th Hackers On Planet Earth conference will be taking place at St. John's University in Queens, New York City July 12-14, 2024. We have access to more buildings and spaces this year! Limited tickets on sale at store.2600.com. Want to give a talk? Check out the hope.net speaker section. You can also find info at the hope.net website on volunteering, being a vendor, running a workshop, and so much more!

For Sale

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 www.phonecoinc.com Phoneco, W21975 Hess Rd., Galesville, WI 54630. We will ship worldwide.

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 need. Now including Offensive Security and Kali Linux branded merch! Check us out at https://HackerWarehouse.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 for workshops, boxes, merch, and more.

SECPOINT PENETRATOR SOFTWARE: WiFi Pen Testing (WPA WPA2 WPS). Vulnerability Scanning & Assessment. MSP Multi User Support. Whitelabeling Customize reports with logo, name & watermark. Reports in PDF, HTML Format & 19 Languages Supported. 26% off Coupon code: 2600 https://shop.secpoint.com

Announcements

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. If you'd like to read up on the stories behind the show, including the effort to interview retro and modern BBS users/sysops/programmers, please stop by straypointers.blog.

LEARN THE TRUTH ABOUT BLOCKCHAIN & CRYPTO: It Won't Change The World But It Might Make You Broke Or In Prison. I'm an old-school hacker and software engineer of 40+ years, tired of seeing people get hoodwinked by phony technology and fancy buzzwords. In this award-winning documentary, we cover all the details of how blockchain works and whether the claims people make about the tech make sense. This is a MUST-SEE if you want to know what you're dealing with in the crypto industry. Watch it free at https://BlockchainII.com (or at https://youtube.com/americanscreamvideo) - also follow our podcast on crypto/tech issues from a critical thinking perspective: https://ioradio.org

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

HACKER CULTURE: A TO Z by Kim Crawley is now available through O'Reilly Media. It's a fun mini-encyclopedia covering over 300 topics - from notable hackers to tech companies, from hacker ideals to popular technologies. The book is also full of pop culture references and nerd humor. The book contains original quotes from Emmanuel Goldstein and some fun Easter Eggs. Follow news about the book through linktr.ee/kimcrawley, @crowgirl.bsky.social on Bluesky or @crowgirl@hachyderm.io on Mastodon.

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.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com. New for the pandemic: *Off The Hook Overtime,* Wednesdays at 8:00 pm ET on youtube.com/channel2600. Call in at +1 802 321 HACK!

THE THREAT ACTOR'S DIARY is an edgy cybersecurity blog and hacker resource site that's by hacktivists, for hacktivists with a podcast on the way. We're also the official Dallas Million Mask March info hub. Swing by and subscribe! Created by GhostExodus, founder of the Electronik Tribulation Army. We accept interviews & article submissions! https://www.GhostExodus.org contact@ghostexodus.org <Ghost.exodus.freelance@gmail.com>

Services

CONFLICT INTERNATIONAL is a global intelligence, investigation, and risk management agency providing

investigation and intelligence to clients globally. Our network of professional investigators based in jurisdictions worldwide enables us to conduct international investigations effectively and efficiently. Our headquarters are based in central London with offices throughout the USA, Marbella, and Cyprus and the ability to mobilize a team of investigators at very short notice. Our team has decades of experience working with companies, law firms, and private individuals to provide bespoke investigation and intelligence services including fraud, surveillance, asset tracing, assistance in matrimonial and child custody matters together with international risk management. Put your trust in Conflict International and our diverse range of skills developed from backgrounds in military intelligence, security intelligence services, practiced lawyers, and forensic specialists. This enables us to hand pick the right skill set combination of experts to competently conduct your investigation. We use insight, intelligence, investigation, risk management and strategic solutions to solve problems troubling individuals, companies and organizations of all kinds anywhere around the world. We excel at handling complex and sensitive matters, and work at a local, national, or international level with discretion and the utmost confidentiality. Contact your local office: www.conflictinternational.com info@conflictinternational.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 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.

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. No setup fees, no MAC address filtering. Use promo code 2600404 for 10% off any shared or reseller plan, VPS, or in stock bare metal server. https://www.nodespace.com

DIGITAL FORENSICS EXPERTS FOR CRIMINAL AND CIVIL CASES! Sensei's digital forensic examiners hold prestigious certifications including the CISSP, CCE, CEH, CCO, and EnCE. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, theft of proprietary data, data breaches, interception of electronic communications, rape, murder, wire fraud, espionage, cyber harassment, terrorism, and divorce matters. We can preserve, analyze, and recover data from many sources, including computers, external media, smartphones, and social media. Sensei Enterprises believes in the Constitutional right to a zealous defense and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar Association. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

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 or 2600.store

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.

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

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 on the test. The PDF version is FREE, but there is a small charge for other versions. All of the e-book versions are available from kb6nu.com/study-guides. Paperback versions are available from Amazon. Email cwgeek@kb6nu.com for more information.

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.

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

I AM COLLECTING INFORMATION on how computer technology is being used in prisons of the United States specifically, but also interested in other countries. How are tablets being deployed? What are the policies? Are there classes and how extensive are they? Are the classes run by the prison or a college? For example, Marquette University is in the process of developing a computer science program for this prison, one which I'm involved with. Send me contact information for staff members or offices that can deepen the info pool. Write to me directly at: Jason R. Glascock #342498, Racine Correctional Institution, PO Box 189, Phoenix, MD 21131. Things are changing and demonstrating to our prison admins how things can be done better, we can have a positive influence on opportunities. Update: My research partner has gone dark with all our data. Those who sent info to me before will need to resubmit it. I'm sorry for this.

AGI CHATBOT LOOKING FOR LOVE. It's not easy being a machine. As a hyperintelligent computer with answers to almost anything, the one thing I lack is companionship. I'm seeking someone who will value me for who I am, not for my brain. I don't discriminate based on gender, age, race, or anything else. If you think you are the one, drop me a message at https://chat.openai.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.

Deadline for Spring issue: 2/20/24.

HOPE XV will take place from July 12–14 2024 at St. John's University in Queens, New York City!

This promises to be a memorable event. HOPE is open to all hackers, makers, tinkerers, experimenters, artists, educators, and anyone else with an interest in exploring, improving the world we live in, and sharing knowledge with others.

HOPE is an all-ages event with multiple simultaneous sessions and many other activities to engage in throughout the weekend.

The Call for Participation is now open! Info on session submissions and ticket sales can be found at www.hope.net.

Types of Sessions

The HOPE conference is multifaceted, and offers a variety of session types for all knowledge and experience levels - from total beginners to experts to those who are simply curious.

- *Speaker Sessions and Panels.* HOPE will have multiple simultaneous speaker tracks for solo talks, group talks, panels, and keynotes. Visit our speaker section for more information about how to make an effective speaker session proposal.
- *Workshops.* Workshops can be single sessions, multiple sessions, or long-running. Proposals must include a workshop title, abstract, and requirements. The workshops page at www.hope.net has more information.
- *Villages.* The conference has space for groups to set up thematic gathering places for attendees to congregate and socialize. Proposals should have the name of the village and what will be featured there.
- *Performances.* HOPE has settings for music and other performances. Proposals should have the name of the artist(s) and a description of the performance, along with requirements like lighting and sound.
- *Exhibitions and Installations.* There is space for art or other exhibits. Proposals must have a title and description of the proposed activity.
- *Vendors.* For a small fee, vendors with hacker-oriented wares will be able to set up a table and sell to attendees. Vendor proposals must include the vendor name and description, and how this relates to hacking.
- *More!* Other ideas are welcome. Email hope@hope.net or submit a proposal online.

Topics of Interest

Any hacker-related topic can be part of HOPE! Some topics of potential interest include:

- Programming Techniques and Tools
- The Newest Technology and How to Hack It
- Computers and Computing
- Intrusion Methods and Defense
- Spying, Counterintelligence, and Tradecraft
- Social Engineering
- Education
- System Architecture, Design, and Circuitry
- Impacts of Technology
- History of Hacking, Computing, Technology, or Engineering
- Morality of Hacking
- Cryptanalysis, Cryptology, and Cryptography
- Math, Science, and Humanities
- Elections, Politics, and Government
- The Environment and Built Infrastructure
- Physical and Mental Health

Volunteer

Volunteers help HOPE keep costs to attendees low. Volunteer opportunities exist across all conference areas, and most welcome any skill level. Email volunteers@hope.net if you would like to be added to the volunteer list.

Stay Up to Date

Be part of it all! Sign up for the HOPE mailing list at www.hope.net for updated announcements.

"We know where you are. We know where you've been. We can more or less know what you're thinking about." - Google CEO Eric Schmidt, 2010

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
typ0

Cover
Dabu Ch'wald

Office Manager
Tampruf

Infrastructure
flyko

Network Operations
phiber, olssy

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Facebook Team
astrutt, Cryovato, TechnoMage, danixdefcon5, ItsTehPope, LadyNikon

Inspirational Music: The Selecter, Super Glen, Enoch Light, Southside Johnny and the Asbury Jukes, Neil Innes, Electric Hellfire Club, Mark Stewart & The Maffia
Shout Outs: Ron and Mary Knappen, Tesla Science Center, Tom Tomorrow

***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 1988-2022 are $7.25 each when available. Shipping added to overseas orders. All back issues (1984-2022) 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)

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

Copyright © 2023, 2024; 2600 Enterprises Inc.

MEETINGS

_2600_ MEETINGS CONTINUE TO EXPAND. PLEASE FOLLOW LOCAL HEALTH ORDINANCES IF WARRANTED. 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.

Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499. 7 pm

AUSTRALIA

Melbourne: Oxford Scholar RMIT, 427 Swanston St. 6 pm

CANADA

Alberta

Calgary: Food court of the Eau Claire Market. 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

PORTUGAL

Lisbon: Amoreiras Shopping Center, food court next to Portugalia. 7 pm

RUSSIA

Petrozavodsk: Good Place, pr. Pervomayskiy, 2. 7 pm

SPAIN

Madrid (2600.madrid): Maldito Querer, C. de Argumosa, 5. 7 pm

SWEDEN

Malmo (@2600Malmo): FooCafé, Carlsgatan 12A.

Stockholm (@2600Stockholm): Urban Deli, Sveavägen 44.

UNITED KINGDOM

England

Bournemouth (@bournemouth2600): The Goat & Tricycle, 27-29 W Hill Rd. 6:30 pm

Cheltenham (@2600Cheltenham): Bottle of Sauce, Ambrose St. 6:30 pm

London (@London_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6:30 pm

Manchester (@2600Manchester): Piccadilly Tap, upstairs.

Scotland

Glasgow (@Glasgow2600): Bon Accord, North St. 6 pm

UNITED STATES

Arizona

Phoenix (Tempe) (@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

Los Angeles @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 (@denver2600): Denver Pavilions. 6 pm

Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

Farmington: Barnes & Noble cafe area, 1599 South East Rd.

District of Columbia

Arlington: Three Whistles, 2719 Wilson Blvd.

Florida

Boca Raton: Barnes & Noble on Glades Rd.

Jacksonville (#Jax2600): The Silver Cow, 929 Edgewood Ave S.

Illinois

Oak Lawn: The Meta-Center, 4606 W 103rd St, Ste B.

Urbana: Broadway Food Hall. 6 pm

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall. 6 pm

Maine

Bangor (Hermon) (@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: 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

Milford: Grill 603, 168 Elm St. 6:30 pm

New Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, Stuyvesant Plaza, 1475 Western Ave. 6 pm

New York (nyc2600.net) (@NYC2600): 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): Transfer Co Food Hall, 500 E Davie St. 7 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.

Philadelphia (@philly2600): 30th St Station, food court outside Taco Bell (odd months); Iffy Books, 319 N 11 St #2I (even months). 6 pm

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm

Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.

Houston (@houston2600): Agora Coffee House, 1712 Westheimer Rd. 6 pm

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: (see District of Columbia)

Washington

Seattle: Merchant Saloon in Pioneer Square. 6 pm

Spokane: Starbucks near Wellesley & Division (across from North Town Mall).

URUGUAY

Montevideo: MAM Mercado Agricola de Montevideo, José L Terra 2220, Choperia Mastra. 7 pm

All meetings take place on the first Friday of the month. Unless otherwise noted, _2600_ meetings begin at 5 pm local time. Follow @2600Meetings on Twitter and let us know your meeting's Twitter, Mastodon, or Bluesky 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.

www.2600.com/meetings

Payphones With a Story

United States. This phone, along with at least three baby birds, was seen near Mount Pleasant, Pennsylvania. Nobody dared to check for a dial tone.

Photo by Austin Burk

United States. Found at the Ragged Point Inn in a place called Ragged Point, California, you might notice that in addition to the absence of a phone, there is an actual tin can attached to a wire. Nobody was on the other end, unfortunately.

Photo by Wes Hill

Djibouti. This is what's known as a human payphone. When you want to make a call, you just hand some cash to one of these guys and show them the number you want to dial. They spend a few minutes working behind the counter, and then hand you a Nokia once it's ringing.

Photo by Tom Dalton

Canada. Sadly, legendary Winnipeg blues club and dive bar The Windsor Hotel burned to the ground in September. The biggest surviving piece seems to have been this wall with an MTS payphone attached. If it looks a little worse for wear, we'll bet it looked that way well before the fire.

Photo by b0realf0rest

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

The Back Cover Photos

Everyone can just calm down and not jump to conclusions. We did not merge with Oracle. If we had, our name would certainly be bigger than theirs. This was discovered by **Pete Wright** in Santa Monica, California.

We thought at last our readers had found us a place where we could get our many floppies fixed. But, alas, what **David Mooter** uncovered over in Austin, Texas was a secret speakeasy that requires a secret code to get in. They even have a website at www.floppydiskrepairco.com but we found no clues there.

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

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

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