Volume Thirty-Eight, Number Two
DIGITAL EDITION

2600

The Hacker Quarterly

Foreign Payphones

Greece. Seen near the Acropolis of Athens. The phone company is Cosmote (OTE) and this phone appears to be from the 1990s. It accepts prepaid cards.

Photo by Major League Wiffleball

Ukraine. This was found in the town center of Dnipro. Even though you'd likely have a lot of trouble using it, this seems like a relic that should never be removed.

Photo by Floppy Phreakaka Solar Angel

Tanzania. Seen at the airport in Dar es Salaam. Located right next to the mosque where you have to be careful not to step on people's shoes when making a call.

Photo by Richard D

Zambia. Found at the airport in Ndola. It accepts cards and still seems to be in service.

Photo by Richard D

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 (Do not send us links as photos must be previously unpublished.)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

Ignition

What is Truth?

Most of us are taught fairly early on that truth is subjective. Our disagreements are what define the human race.

Facts, however, are different. They are certainly open to interpretation, but we can't simply make up our own facts to suit the truth we believe in. *Distorting* facts is the more traditional approach towards getting them to back up your conclusions. But everything has its limits.

We're seeing a great deal of fact distortion and fact creation all around us. Behavior that we would expect from toddlers is now commonplace in the halls of Congress and all throughout the media. And while there's definite humor in all of this, we're well past the point where it's gotten super serious - and deadly.

In the hacker world, questioning is our thing. We question authority, we question facts, we question the very technologies that we love. These questions make us stronger and able to design better inventions. The worst thing a hacker can do is simply follow the rules. Exposing the truth, however uncomfortable, is what we're all about. (Ironically, this has made hackers into much more of a perceived threat than they actually are because they like to share the security vulnerabilities they discover, while true criminals know to keep their mouths shut.)

But part of our questioning involves listening to the answers. We all know that we won't always hear the answers we want. So how do we handle it when that happens? There are three ways.

- We can accept what the facts tell us.
- We can ask more questions.
- We can assume the facts are wrong and try things from a different angle.

All three of these approaches are acceptable to a point. A combination of the first two is generally what we've had the most success with. It's not healthy to just accept things because that's what you're told. There will always be more questions to help clarify what it is you're seeking to understand. This process is a progressive one, where more is learned and a conclusion begins to come into focus. The third approach isn't necessarily a bad one, especially if you believe that you're not being given all of the information. However, if it becomes your default reaction, or if you find yourself going back to this repeatedly, it's generally not a good sign. It's indicative of people who already have their version of the truth defined and are looking to shape facts to suit that truth.

It's particularly annoying to us and to many in the hacker world to be told that we're not asking enough questions or, worse, that we're in league with governments or pharmaceutical companies because we've concluded that the vaccines against the deadly COVID-19 pandemic are safe and effective. Those who accuse us of such things are angry that we haven't shared their particular version of the truth. They ignore the fact that we've looked at the evidence, analyzed the science, and listened to the experts who have devoted their lives to this sort of thing. And it's clearly not the only fact they've ignored.

Throughout this crisis, there have been people who refused to believe it was real. They wouldn't wear masks. They wouldn't observe social distancing. They assumed the whole thing was some sort of global conspiracy whose alleged goals have never been clearly explained. And now, with a death toll of over 600,000 people in our country alone, more than four million worldwide, their continued attempts to minimize this horror are despicable. If it continues, we will wind up right back where we started with the very real

possibility that the next strain will be even worse.

The vast majority of the hacker community gets this. We analyze situations constantly and make choices based on the evidence in front of us. We *never* follow blindly. Those who make these accusations want us to do exactly that: follow *them* blindly without credible evidence. That won't happen in our community and we need to do everything in our power to make sure it doesn't happen outside our community. This has nothing at all to do with politics, religion, or anything other than science and logic. However, if a political or religious ideology attaches itself to illogical and deadly thinking, that's entirely of their own volition.

As with anything, facts change over time. We've heard the advice from experts evolve from month to month. This happens when a situation is in flux and we learn more about what's actually occurring. Strategies get modified as our knowledge base grows. To point to this as some sort of evidence of wrongdoing is highly irresponsible and could actually encourage important updates to be downplayed due to fear of misinterpretation. That's not a healthy environment.

Possibly the most disturbing part of all this is hearing of "breakthrough" cases where fully vaccinated people come down with - and even die from - COVID-19. This, incredibly, leads some to conclude that the vaccine doesn't work and isn't worth getting. In actuality, this is happening in places where the vaccine rate amongst the population is low. That increases the chance that *anyone* can get the virus, even those who were vaccinated, albeit at a much lower rate. But it's not a zero rate. So people who have done the right thing are literally losing their lives because of people who refuse to look at the facts and listen to the experts. And, if that's not enough to be upset at, consider that the longer this virus hangs around, the more likely it is that a variant will emerge that is immune from the vaccine entirely and possibly even more deadly. This is what ignorance and misinformation can produce.

We need to use every skill at our disposal to fight this and save lives. We want this dark period to end once and for all. We want our normal lives back. We saw things improve when guidelines were followed. We saw drastic decreases in cases once the vaccine arrived. All of that is at risk and for no reason other than some of us are susceptible to being manipulated into espousing a truth that isn't supported by facts. Our social media has the ability to be socially responsible. But it's ultimately up to us to make sure they are.

We have the power to steer things in the direction we need to go. And *that* is the truth.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2021. 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	24875	24750
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	5621	5260
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	17994	17900
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	23615	23160
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	114	127
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	899	921
E. Total free distribution	1013	1048
F. Total distribution	24628	24208
G. Copies not distributed	247	542
H. Total	24875	24750
I. Percent Paid	96	96

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

More Privacy and Better Security Through Email Diversification

by Elite Bulbe **elite.bulbe@yahoo.com**

In this article I will put forth some ideas I have been trying out for myself over the last year. I won't claim that what I'm suggesting here has not been thought of before. I do hope you will think about how you use your own email, and gain insight into how everyday tech-savvy folks can increase their privacy and improve their security by changing how they use their email.

My main goal has been to increase my privacy. As it turns out, the method I have chosen can also improve my security as well.

My plan was to reserve a new domain name and then create a slew of new email addresses under this new domain. For security purposes, I will probably end up creating five or six email addresses which will only be associated with one company or account apiece. For example, if my credit card company gets hacked, the hackers only know the email address associated with my credit card, and not the ones for my bank or cloud storage. On the privacy protection side, I will create a series of email addresses for different facets of my life.

All of these new email addresses will funnel all email into a single secret master email account, using something called an email alias. Thus emails to jekyll@myprivateida.hu and hyde@➥myprivateida.hu would all end up in the inbox of secretsquirrel@myprivateida.hu.

Do not be fooled by the suggestion you may see on the Internet that one can use the "plus" method to create email aliases for this purpose. With Gmail and several other email providers, you can add a plus sign and then concatenate letters/numbers after the plus to create a "different" email address which funnels into the original email address. Thus email sent to example+porno@gmail.com and example+reborn@gmail.com both end up in the inbox for example@gmail.com. Problem is, from a privacy and security perspective, this does not really create new email addresses that are unknown to your adversary. The plus sign makes very clear what the root email address is. Everybody in the business knows about this system, so marketers and spammers undoubtedly strip off anything after the plus when matching up email addresses from different locations, so there goes your privacy as well!

My Situation

I have owned a number of domain names over the decades, some of which are even being used. I try to run most of my email through two email addresses split between two of these domains. One email address and domain name is very publicly me. It is has my business name, and this is the email address I give out to human beings I know. The other email address is not used for personal stuff. This one I use when I do business online, or almost anytime I need to register online for commercial or computer forums, git, etc. Oddly enough, the first email was supposedly going to be kept spam-free, and the second one was expected to develop quite a following among spammers. Sadly, a dramatic reversal has occurred because of my procrastination. I left my email and phone numbers up to be scrape-able by web-crawlers on the business website. (Actually, I was not as stupid as that, but the spammers' web-crawlers are now presumably running JavaScript and obtaining my previously obfuscated email address.)

Every five years or so, I try to review and "level-up" my security and privacy. For this "five year plan" level-up, I want to do several things:

- Add two-factor authentication to accounts which warrant it. (I've already done it for most of my financial stuff, but not for some important web accounts, such as the cPanel account for my web hosting company, or for the DNS registrar I use.)
- Improve my security against random hacking. My emphasis is not going to be to prevent a determined nation state level hacker from being able to read my email. I only want to secure my "stuff" against hackers trying to take advantage of my digital online belongings or trying to get my money. I am not an activist, and I am hopeful that the NSA and CIA have only slightly elevated interest in my doings. Just cranking up Tor, subscribing to *2600,* or opening a non-work-related VPN connection probably puts you on some sort of list. I just hope it does not make them think they have to hack into my accounts (yet).
- Start to gain some control over my privacy against the Big Tech Five Eyes overlords and their ilk: Google, Facebook, Apple, Microsoft, and Amazon (as well as your ISP and DNS providers).
- Re-compartmentalize and reassign email addresses to specific purposes.
- See how hard this will make it for me when I add this extra overhead into my email use.

Considerations for Current Owners of Their Own Domain Names

I decided I would need a new domain name and a new hosting provider. Owning your own domain name has both pluses and minuses. To start off with some negatives: This will cost you money. The DNS registration is going to run you at least $10 a year, and then you are going to have to pay a hosting company to host your email, which will be minimum $25 to $35 a year and can shoot up to $100 to $200 a year. My goal was to keep it under

$200 a year. You are also supposed to give your registrar your real name and address. If you do not, they could actually steal your domain name from you, if you had one worth stealing, and it might be very difficult to prove that you owned it. I suppose the way to get around this would be to create a shell company and have it buy the name.

On the plus side, having your own domain name will give you portability and long-term stability. If I don't like my hosting company, I can take it elsewhere without having to re-notify everywhere I have registered it with. It also makes you feel like you are beholden to no one. It's your own little private Idaho, you can do things your way, but it's on you to pick your vendors well, and do your own due diligence security-wise, like security precautions that would be done for you, or that you could ignore if you were to use Gmail. Domain name owners free themselves from the kind of privacy invasion we can all assume comes to those who depend on email, calendaring, address-book sharing, and messaging provided by the likes of Hotmail (and outlook.com, live.com, skype.com, etc., all Microsoft), Gmail, Yahoo, Apple, or your ISP.

Now, why did I just not use one of the domain names I already owned? It would be cheaper for one! Less complicated as well. Problem was, from the privacy angle, if I set up this new domain under my old account, it would share its IP address with existing domains with publicly facing links to my actual person. Ten to 20 years ago, I started paying my current hosting company for a private IP address. Typically, if you own a domain name through a hosting company, your domain is hosted on a shared host server along with hundreds of other folks or companies like yourself. Usually each server host will be assigned its own IP address to be shared by all of the hosted accounts on that server.

Back then, it made sense for me to pay extra for my own IP address, and stop using the shared address that all of the other hosting customers on my server were using. If you have a private IP address, you were supposed to get a better search engine ranking for your website. In addition, your email was less likely to get tarnished by association if any of the other domains on the shared host ended up on a spam blacklist. Even if all of the other domain name owners were legit, if any of their accounts got hijacked by spammers, it could negatively affect you because the domains for your email would share the IP address of a spammer and get assigned a bad SpamAssasin score, and thus end up in your receiver's spam folders instead of their inbox.

Now owning a series of domains which were associated with one another by a single IP address meant that it was relatively easy to cross-link my public-facing email addresses with the other addresses I had. I checked with the hosting company I was using, and to move up to a plan that would allow me to assign a separate IP address to each domain would be too expensive. On top of that, I prefer that my new domain name be on a shared host anyway, so that it shared the same IP address with hundreds of other random hosted domains.

This is one of the few advantages of using Gmail: it does allow you to disappear into a really big forest. Unfortunately, then Google themselves gets their beak into your underwear.

If you own your own domain name and never paid for a private IP address, you are probably fairly isolated from a quick connection being drawn between one domain on the account and another, though if your life depends on it, don't go by my word on this! I'm just a security and privacy enthusiast, not an expert.

So, How to Do This:
Register Your Domain Name

First you must register your new domain name. You will want to do this using a registrar that offers WHOIS privacy, which in my opinion should be free if you are already paying them for the domain. A lot of registrars will practically double the yearly cost of registration just to provide this privacy. With little knowledge about this, I suggest either `porkbun.com` or `InternetBS.net`. I have not used Porkbun, but they are inexpensive, U.S.-based, and possibly more trustworthy than InternetBS.

InternetBS has the advantage of being based in the Bahamas, though who really knows where they store your account bits. It looks like they use Google Analytics, so there is that, though I think it's unlikely that Google will have written custom code to capture the names of your domain(s) you have registered here along with your name and address collected elsewhere. Note that InternetBS in 2012 had a lot of shady business going on, being the registrar for one-third of all bogus pharma websites on the Internet. I still have not figured out whether doing business with this sort of company means they will protect your identity from the muggles, or if it just means they're more likely to sell you out for little money. It does mean that I have even less faith in the truth and accuracy of their privacy policy as opposed to other more well-known companies. Internet.BS was bought by CentralNIC of London, and I assume that they would hand over your identity in a heartbeat if presented with a court order from any of the Five Eyes, since they literally provide an email address for law enforcement inquiries front and center on their website.

As a side note, I am baffled by the trust reviewers place on published privacy policies. As if there is any real penalty for these companies to lie on their websites! Come on! Its a Wild Wild West out there

that only a libertarian could love. I think the wiser assumption is to assume that every company is completely untrustworthy, and then figure out how to work with that.

Sign Up With a Hosting Company

Once you have got a domain name nailed down, you have to get it hosted somewhere. I do not recommend using the registrar for hosting, though many of them will offer the service.

This is where I went into analysis paralysis.

I needed a hosting plan only for mail. It was OK if they offered web hosting, I just was not going to use it. I wanted the ability to have 30-40 email addresses all alias or funnel into a single email account. I wanted to be able to also use the hosting company's own generic domain name for "burner" email addresses that I could leave behind if I changed hosting companies, but would be even more private. That would be where you put accounts for your embarrassing prawn habit or your communications with bare-chested guys with face paint and wearing buffalo heads.

I did not need a lot of storage space, as most or all of these email addresses were going to be low-traffic, and require almost no long-term storage. Finally, I decided that I wanted the hosting company to provide a mobile app-based method of accessing my admin controls and email. It was a nice-to-have to also have email-client access using IMAP/POP and SMTP, but not required. (I changed my mind on this later after signing up with my final choice.) In addition, unlike many folks in this magazine, I did not require or even want email encryption. Honestly, I couldn't care less if someone at the hosting company could read my emails. Too boring! On the other hand, if you are an activist or person of interest, this may be the single most important factor in selecting a hosting company.

Lets revisit the whole question of app vs. email client vs. web-based email methods. It's probably just me, but I hate web-based email. I like using an email client, in my case, Mac Mail. Unless I am on vacation, I tend to avoid reading email through a client on my phone. Just be aware that if you are like me, and you like using a client, you have to be very careful to not leak your home or mobile IP address when you are sending email.

Here is where web-based email is better. Web-based or a vendor-provided app is less likely to leak your IP address. If you are using an email client, I think you had better be using a VPN, or you risk leaking your location. Check for IP leakage by sending email from a free test account using the method you will be using before signing up for their paid tier of service. You will find the IP address of the sender after the "Received: from" line in the header. Look at each one - the email is usually forwarded several times. It is the originating sender that will have your IP if it is leaking. You can use a web-based email header analyzer such as `www.gaijin.at/en/tools/➥e-mail-header-analyzer`. Just note that when you paste your email headers into that, there is the chance that `gaijin.at` themselves are recording the to and from addresses/IPs, so if you are super-paranoid, get there using a VPN and use a burner email address.

I am always worried when I am using a website through my phone that I will leak info unintentionally. I just don't have as much knowledge about what is happening or control over my phone network-wise, so I decided that I would prefer to have a vendor-provided app instead of using their web-based interface. In general, even being careful on my Mac is hard. Even if I ever get around to using VPNs more regularly, I just find it's too easy to forget whether I am operating "in the open" or "in the pipe."

Final Hosting Related Steps

So once I had an email hosting vendor, what next? I had to point the DNS MX record for my domain to the email hosting service. Look on the email hosting website for the text strings needed to point to your domain, and then look on your registrar's website for instructions as to where to modify the DNS records with this info.

You can then start creating new alias accounts on the hosting site, and creating new accounts on the places on the web you do business with. Just remember: if you already had an account with someone, you'll often want to create a brand new account if possible instead of changing your account profile's email address. I don't know if anyone is tracking data at this level yet, but if you use the same phone number, address, name, or credit card number on the new account, that might also leave a trail of breadcrumbs leading back to the well-known digital persona in your previous incarnation.

Pick New Email Addresses

...So the whole point of all of this was to get a whole bunch of new email addresses. The ones for financial and important network accounts will be created one-per-destination. If my credit card email address is discovered on IveBeenPwned.com, I can be secure in knowing that: 1) I don't have to be concerned that the adversary would have much luck guessing the email address for my bank account or my web-hosting cPanel; 2) When such a leak is discovered, I can take the more prudent action of just changing the email address used for the profile/recovery of such an account instead of just changing the password. Since the email address is only used for this one account, it's no biggie to allocate a new one for this one account, whereas in the old way of doing things, it would be way too much work to create a new email account and notify every place it got used with the new one.

Since the purpose is to make it difficult for

an adversary to guess the email account name based on the leak of any one email address, you should choose wisely. Do not go off and create capitalone@MyPrivateIda.hu, because if it leaks, it will be easy for them to guess that mybankname@➥MyPrivateIda.hu is the email address for your bank. It goes without saying that you will never use the email address which "owns" this account, and to which all of these aliases funnel down to. That should stay secret.

Creating a separate email address per destination for run-of-the-mill non-secure accounts would be a lot of work, plus many of these mail hosting providers charge quite a bit of money for extra aliases.

So, for privacy-related use, I created basket accounts which would get shared for whole categories of accounts. Thus I created one group account for each of: media, gaming, news reading, GPS/navigation, travel, retail/shopping, non-critical cloud services, health care, etc. You make up your own set of categories. For example my media email is given out to Netflix, music, and other related streaming accounts. I imagine my medical/dental account will be used for everything including insurance. I don't really care who knows what I've got. If you do, you might want to split them up; just realize you could make things difficult for yourself when the hospital your doctor has admitting privs with tries to use the same email address for itself and your doctor. The same is true for a bunch of other categories. One address gets inherited or passed on to the next place.

Lots of IoT devices need an email address to register with as well. This is one area where I think there are some serious privacy issues I've never seen discussed anywhere. I'm thinking of my smart garage-door opener and my sleep number bed. Just think about what you are giving away when you use those two. Some corporation gets to keep track of when you come and go from your house, and when you are away on vacation. With the bed, they can probably figure out what your sex life is like and a lot of other personal stuff. This is not a stretch, since that sensor is sensitive enough to capture my heart and breath-rate, while it is measuring how much I toss and turn at night. If it can tell when you are awake or asleep, don't you think they can figure out what sex position you are using with your partner?

Calendaring and Address Books

I almost forgot. When you sign up for email hosting, you usually also get cloud-based calendaring and address booking. (I don't even mention it in my criteria below for hosting companies.) I cannot write this up yet as I have not gotten myself off of the big "G" for these two sources of privacy leakage. Of the two, the address book privacy issue is the worst in my situation. I've got 700+ people in my address book, often with a full first name and last, with phone number, email address, and snail mail address. This is a huge privacy leak, and I need to write in the future about my experience of cutting this over as well. I will say, I already create incomplete or obfuscated snail mail addresses for new entries.

Mail Hosting Companies to Consider (in Alphabetical Order)

The final list of vendors I came up with for email hosts is surprising (even to myself), but I think anyone reading will find a host that provides the right combination of cost and features you require. This list spans a wide set of needs. They all satisfy my desire to keep the yearly fees down. If you could care less about usability, but want encryption security, there are several. If you just want easy-to-use cheap mail hosting with possibly suboptimal privacy and security, I got that too. (By the way, I think there is a lot to be said for hiding in plain sight. I think using Proton, Tutanota, or CTemplar immediately puts you in some sort of category.)

CTemplar - This one was in the running until the end. They responded right away when I asked for a referral code, they had a nice looking Android app, they are based in Iceland, they seem to be new, and, as a relatively new vendor in the market, I saw them as "the underdogs." This sorta cuts both ways though, as it means that the forest of other clients to hide in is smaller - instead of having ProtonMail's ten million users, I suspect their user base is still well under one million. I think my main problem in the end was subtle. I found I could not grab an unmunged text version of the email headers from incoming email. They had prettied it up, and made it impossible for me to select in a single cut to paste into a website I use to analyze email headers. Although they do not allow IMAP, they do support email forwarding.

FastMail.com - If you are a security/privacy nut, you are probably surprised to see these guys on my list. They have the advantage of being large, and based in Australia. Aside from that they are not likely to be trustworthy, either for privacy or security reasons. Given the low bar your average user in the real world (not you, of course) has for privacy and security, these guys will not lose any market share if it is reported that they get caught with an egregious privacy or security blowout. ...But. They give you a pretty big forest to hide in. They have a huge assortment of vanity domain names you can use when you are not using your own domain names. If I were going to be looking for an inexpensive way to do this, I might go with these guys for a privacy-centric solution. $36 a year and 600 aliases. I wish Tutanota, CTemplar, Proton, etc. would give out aliases that freely. Not bad!

ProtonMail - The Ten Million User guerrilla in the room. According to a `digdeeper`.

neocities.org write-up on them, they are problematic. Strangely, I finally decided against them because my password manager did not play nice with the way they encrypt my emails with a different key from the password I use to access my account. Yeah, yeah, I've ended up with another provider who I do not even have the encryption turned on for! I also was bewildered by their smorgasboard of plans add-ons. It seems to me like many, they charge too much for extra aliases. If you want to send secure encrypted emails to other folks, this is probably the one to use. There are already tons of users on it, and when it comes to easily sending encrypted email, you can either spend a lot of time messing about with PGP, or you go with a vendor where you only send emails to other users of their service. Even the creator of PGP no longer thinks PGP works well for email, and is looking for a better solution. ProtonMail has some sort of Bridge app for paid users to use IMAP on some of the most popular email clients. I don't think they allow auto-forwarding.

TheXYZ - A bit like Fastmail, but probably more secure. They have an app. They are based in Canada, aye? They offer unlimited email aliases. Inexpensive.

Tutanota - This was the one I kept coming back to. Based in Germany, they have millions of users. It seems like they got into the business for privacy protection as much as security. Reasonably usable app, relatively inexpensive. They charge more for the number of aliases I will need, but not that much more. The cons are that they have a terrible name IMHO.

If I were worried about nation state adversaries, I would probably pick ProtonMail or CTemplar.

The Runners Up

In the list of runners up, two looked like comers, but they require you get a referral from an existing long-term customer: Countermail and RiseUp.

CounterMail - They claim if you do not know anyone to get a referral code from, you can email them, but their emailer just kept bouncing my request. Don't waste my time, you jerks!

Riseup did not give you a way to sign up if you did not know an existing customer.

CripText - Out of Miami, they look expensive.

EPrivo - Possibly based in Massachusetts, no storage.

Cotse.net - This looks like a little mom and pop outfit with personal service. I discovered them after I'd signed up with Tutanota, just as I was finishing up. I'll probably look into them more. They are from Worcester, Massachusetts. That's "Wuhstah, Mass" to you non-New Englanders!

StayPrivate

PrivateMail - No bring-your-own domain?

Experience Using Tutanota

I finally decided on Tutanota, but based on what I have found since paying them, I will not be renewing the service unless they add the ability to create an email account which can forward an incoming email (preferably to two different external accounts). It's becoming clear to me that for the ease of use, a service that allows IMAP access should be a requirement. My partner will put up with a certain amount of craziness on my part, but there is no way I could persuade her to use a special app just to read certain email messages. My partner and I share access to an EasyPass account, and they only allow one email address to be used to send out notifications, etc. I want to use a independent and unique email address which would forward to both my and my partner's accounts. You can't do that with Tutanota.

As time wears on, I am finding it tiresome to have two different piles of mail to look through. I have already twice spent minutes searching through Mac Mail before it finally dawned on me that it's in Tutanota. I think IMAP should be a requirement if usability is at all important to you and you are like me, unwilling to completely jettison your old email addresses.

I should also mention that funneling all of my current email addresses through Tutanota might be one way to get all of my mail in one pile. If I did this, I would probably create in my case two accounts, maybe even using Tutanota's own vanity domain name, so that if I do reply, I am not revealing my "main" domain name to users of my older domains.

From an ease-of-use perspective, creating a new alias seems to be a bit awkward too. I think I counted eight taps from opening their app to being able to tap on the "+" to create a new alias. This includes the craziness of selecting the right account of the two I have, then tapping on the "hamburger"/menu icon, tapping gear symbol, then tapping on the exact same "hamburger"/menu icon a second time, which then opens up a menu which exposes the User Management option, after which you will have to select between those two email accounts *a second time*, then scrolling down and having to "open" the alias list to finally see the "+". Clearly, being able to add aliases was not thought to be something a user might do frequently. It's disconcerting to click on the gear symbol two different times, and have to select the right account twice too.

For those folks on the anti-government security end of the spectrum, here is another reason you might want to avoid Tutanota as well. November 2020 news indicates the service is being forced by the German courts to decrypt email messages for an account used to blackmail an auto company. Not a good look for a company depending on the promise that nobody will ever be able to read your emails.

Tricks Learned Along the Way

- I will pass on another interesting tip I've

learned over time. Do not use a single letter email address like z@myprivateida.hu. Over time I've figured out that a surprising number of websites have bugs related to single letter email addresses. These range from badly written regex expressions which prevent you from registering, using what is a perfectly legit email address, to stupid password security tools which prevent you from using your email address in your password (which might make sense for email addresses more than three characters long, but is just idiotic for shorter ones. So it would not allow the password "sQ123!%#" if your email address was either s, q, 1, 2 or 3. As a side note for you hackers and pen-testers out there, I suspect you can use single letter email addresses to break code as well.

- Yandex: You can register with the Russian search engine company for a free email address, and you do not have to provide a mobile number or another email address. Just understand that this email address they give you for free is only good for a short time (probably two months) after which, without notice, they will require you to provide a mobile number for you to get back into your email. This is pretty evil, since at the two month point, most people will have been pretty well settled into their email address, have given it out to lots of folks, and be unwilling to just ditch it without being able to log in one more time.
- You may be thinking that instead of using Yandex, you could just go with one of the well-known disposable email address outfits. Most other major free email services will not accept an email address for "validation" from one of the well-known burner places. (By burners, I mean guerrillamail.com, owlymail.com, gmailnator.com, temp-mail.org, fakemailgenerator.com, 10minutemail.com, trash-mail.com.)
- I live in the United States. I found that I could buy a pre-paid anonymous credit card for cash pretty easily at a local store. Problem is, most (all?) of those cards available through bricks and mortar retail are limited to use within the United States. If you are trying to buy hosting services or DNS registration off-shore, you are going to have to figure out how to use Bitcoin (I haven't) or do something shadier than I was willing to do.
- Even buying a TracFone with cash will make you leave a trail leading home. As I recall, they required me to provide a real physical snail mail address and name during the registration. I do not know what the legal ramifications are for providing false info.

Credit Cards and Burner Phones: Write Me!

This brings up some skills that I still have not mastered, namely what are the ins and outs of using burner credit cards and burner phone numbers if you want to do business online with your brand-spanking-new pseudo-anonymous email addresses? I would appreciate emails from folks who know more about this. Maybe I'll write an article on that next!

Lastly, let me emphasize this disclaimer: your author is *not* a security or privacy expert, just an enthusiast. If you are a high-net-worth individual, or an activist which a nation state or large corporation has taken an interest in, this article was not written for you. I did not cover the steps you need to take to properly protect you from determined adversaries.

References

restoreprivacy.com/email/secure/

digdeeper.neocities.org/ghost/email.html

github.com/ehloonion/onionmx/blob/master/sources/map.yml

riseup.net/en/security/resources/radical-servers

en.wikipedia.org/wiki/Disposable_email_address

Sidebar: A Rant on "Free" and the Original Sin of the Internet

We all must stop with this idea "yeah, but xxx.com offers email for free. Why would I pay for it?" I mean, first of all, look at it this way: how important is email to you? I mean, if you can give it up, great, but if you are like me, you depend upon it (and curse it) daily. If you even pay $50 a year for something you care about (heat, food, water, electricity, and phone service), why would you think you are entitled to free email, social networking, or cloud storage? If you are not paying them any money, then you are providing the company something else instead. Most of the time, you are giving them access to the who, what, and where of your daily life. If you don't mind faceless companies knowing who all of your friends and contacts are, and what gets said in the presence of Alexa and their phones, well, you are different than me.

The fact that the Internet as we know it today has no universally accepted and easily used method for making micro-payments is baked into the protocols and thought patterns of the original techno-elite who designed it. This is the Internet's Original Sin.

Up until the year 2000 or so, everyone designing it pretended that they were these super libertarian do-gooders. Heck no! They were not paying for their newsgroups and email use, they were sponging off of their employers and the U.S.

government. Everyone got their Internet connection from their employer, and the government paid for the DNS system, backbone network, the R&D and standards development, and RFP proposals, etc., etc. used in designing the Internet protocols. Heck, AT&T even came up with the design of Unix and gave it away for free. Some huge percentage of the Internet infrastructure runs some variant of that original Unix. We can thank AT&T and the U.S. government consent decree for that.

Nobody involved really made any effort to fix the micro-payment problem because it was hard, and it would involve the government (shiver... horrors!). And we know nothing good ever comes from government, and corporate high tech is the only human institution which has ever really done no harm and will save us from ourselves. [End sarcasm.]

The U.S. government spends hundreds of millions of dollars yearly minting coins. This is all at a loss, and some of those coins cost more to make than their face value. Why? Because back in the day when things were worth less, and even now for quarters, coins create more wealth during their lifespan than it costs to mint them.

The same wealth could be created by having a working micro-payment system subsidized in the same way by the U. S. government. With it, I could pay for my search engine results and get better search results if advertising were not required to make running a search engine worthwhile. Do you remember how good the results for Google were before they started trying to get their money back on their investment?

Most stuff published on the web would be more profitable at one tenth a cent a page view than any advertising could ever provide, and we could do away with all of our ad-blockers and get faster page loads. What is not to like?!

And forget all of this cryptocurrency utopianism. There is no way that could work for micro-sized payments on a planetary scale. Even Bitcoin right now forces a huge amount of electricity to be expended to keep track of every transaction.

Since it is likely that China will become the dominant government on the planet in the next 50 years, this might be one of the last things the U.S. could do that would have a lasting positive impact on the planet. The only rub is that the FBI, NSA, and CIA would need to be frozen out of their desire to track our monetary use. Yep. Not going to happen.

Three Fundamental Questions

by MasterChen (@chenb0x)

A little while ago, I was asked by a friend of mine to help her strengthen her foundational hacker knowledge. Generally speaking, this meant broad conceptual knowledge about programming, networking, encryption, and security. The hacker mindset goes well beyond any of these categories, but they cultivate a solid foundation.

During our first training session, I had to convey how I think of things in regards to hacking. How can my thought process be simple to understand, convey broad concepts, and remain widely applicable? It was during this first session with my friend that I thought about these three questions.

The first question is "What is it doing?" The "it" being whatever the subject of study is. As an example, we'll use a basic lock. What does the lock do? Well, the lock locks and unlocks under the right conditions; being the proper key inserted and turned, or the correct combination being entered. Whether we are talking about door locks, padlocks, or combination locks doesn't matter. They all have the primary function of locking and unlocking under proper conditions. That is what they do.

So, the second question is "How does it work?" Or, to put it another way, "How is 'it' doing what 'it' does?" Still using the lock example, we know that the lock locks and unlocks, but how? If it's a padlock or classic door lock, the inner cylinder of the lock is secured by pins and springs that are set in place and should only move to a position that gives way when the proper key is inserted and turned. Or, in the example of the combination lock, it stays locked until the tumblers are set in place by moving a dial. This is a short description, but it illustrates the second question.

The third question is "Under which circumstances does it break?" This question can be applied towards both sides of the coin. If we know how it breaks, we... break it, as an offensive play. Or since we know how it breaks, we may know how or where to fortify, as a defensive play. Note that fortification may also include replacing the technology for something better or more up to date. Again, taking the lock example, we know what it does and how it does what it does, but are there ways we can make the lock work without the necessary tools like a key or a combination? A tension wrench and a pick could be a workaround to not having the proper key. A mathematical weakness in the combination allows for quicker cracking. These are conditions under which the original design or intentions break down.

I have tried to think of these questions as a broad perspective on anything that can be hacked; which we know is everything, from the simple to the very complex. If you are a beginner, I hope these questions help guide you in your journey. If you consider yourself to be more mature in your journey, I hope these questions reinforce the solid foundation I am sure you already have!

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I'm supposed to be in Kazakhstan right now, but my original flight routed through both Canada and Uzbekistan, whose borders are (as of this writing in the late summer) currently closed. The pandemic continues to drag on, snarling both business and personal travel, and slowing the fiber deployment I'm working on.

The telecommunications industry is exploding in Kazakhstan. For telephone numbers, the Kazakh numbering plan consists of a three digit area code and a seven digit telephone number. Kazakhstan and Russia jointly administer the +7 country code, making Kazakhstan the only country to have remained in the +7 country code following the breakup of the Soviet Union (note that subsequently, certain breakaway regions of former Soviet republics have rejoined the +7 country code with service provided by Russian carriers). Since it's a small, friendly arrangement, coordination isn't nearly as complicated as under the North American Numbering Plan Administrator. The numbering authorities of Russia and Kazakhstan coordinate their activities under a 2006 agreement, and notify the International Telecommunication Union (ITU) of changes.

The country's numbering plan is interesting, but to me, it's really only a curiosity. Far more interesting is the explosion of mobile phone services in Kazakhstan. There are now five nationwide carriers (Tele2, Altel, Beeline, Activ, and Kcell), so competition is fierce. They offer a dizzying array of plans, including plans for pensioners, hilariously tone deaf plans for students (Beeline's plan offers only 1GB of data and only allows free access to university websites, but not the video conferencing services used for online classes), and multi-device plans that combine a single "unlimited" Internet plan (throttled after 200GB) across a mobile hotspot device and a phone. The cheapest plan from Beeline costs around $5 and offers voice calling only, while the top-of-the-line plan costs about $19 per month. Other carriers charge roughly the same.

Calls are still charged by the minute and, as in Europe, SMS costs per message as well. Some plans come with bundles of minutes, but they are measured in the hundreds, not thousands. This has made WhatsApp the most popular way to communicate. The popularity of encrypted messaging is seemingly irritating to the Kazakh government, which requires real name registration for mobile phones and has been repeatedly attempting to backdoor encrypted communications through the forced installation of a malicious root certificate. It's not clear how this will be ultimately resolved, whether by other means of surveillance or through the implementation of a Chinese-style (and possibly Chinese-built) national firewall.

SIM cards are available almost everywhere. Kazakh people, like Chinese people, enjoy choosing "lucky" or "prestigious" numbers, and carriers capitalize on this by charging more money (up to $700) for numbers that are considered popular. What's an example of a $700 number? +7 771 455 5559, which was for sale as of this writing. Why? It has the number 5 repeated five times in it. When you consider that a line cook or hotel front desk clerk in a second tier Kazakh city makes about $175 per month, this is a truly eye-popping sum of money

for a phone number. Cheaper phone numbers are available for around $1.50 and, frankly, some look pretty good to me. For example, +7 771 207 9200 is available from Beeline at a bargain basement price.

While new SIM cards do work for a couple of days after purchasing them without real name registration, they are deactivated promptly if a passport or national ID card isn't attached. This must be done with the mobile carrier's customer service. Keep this in mind, especially if you buy a really expensive phone number with your SIM card, because you risk losing your number when your service is deactivated! However, deactivation won't happen by surprise. You'll get plenty of helpful messages in the Russian and/or Kazakh languages reminding you to register. Hope you speak both!

In the past, to put money onto your account, you'd visit a mobile phone shop and pay cash. For the privilege of paying your phone bill, you'd have to pay a 10 percent commission (or more) to the shop. Gradually, a Russian company called Qiwi started setting up kiosks. These were more convenient because they operated 24x7 and the kiosks were ubiquitous, but a 10 percent commission was still charged. Finally, Kaspi Bank started offering commission-free bill payments to its account holders via app and kiosk. This service has quickly become one of the most popular ways to make payments, not only to utilities, but person-to-person. It reminds me of how WeChat became the most popular way to make payments in China. It's not uncommon these days for merchants in Kazakhstan to request payment via the Kaspi mobile app instead of cash.

Kazakh payment kiosks, Kaspi kiosk in the middle. These can be used for mobile bill payments, as well as other bill and utility payments.

Mobile carriers are trying to get in on the fun. Beeline, for example, is now offering FinTech-style services and telling its clients to "think of us as a bank." Do you think of *your* phone company as a bank? Maybe in the future you will and, for my part, I fully support this. Just send all of your money to our friendly billing department. We'll helpfully subtract what we would like you to owe, and we'll apply the rest to your account which will be redeemable for future services prior to the expiration date. You know, sort of like an airline voucher. No cash refunds, of course!

And with that, it's time for me to rebook my flights. I'll be resuming a fiber to the home project when I'm eventually able to travel. Yes, Kazakhstan has fiber to the home in many apartment communities, at speeds up to 500Mbps. It's OK, though. The U.S. might catch up by 2048, if the infrastructure bill passes! You wouldn't expect us to invest *our* money, would you?

References

Kazakhstan numbering plan: www.itu.int/dms _ pub/itu-t/oth/02/02/➥T020200006F0001PDFE.pdf

How Mozilla dealt with malicious Kazakh root certificates: blog.mozilla.org/➥netpolicy/2020/12/18/kazakhstan-root-2020/

Fluc Google's FLoC

by kingcoyote

If you're reading this magazine, you're probably aware of the oldest conflict playing out on the Web.

On one side, you have all the people (and companies) using this most amazing communication network to create and share great stuff. Whether it's fan-fiction or software-as-a-service, these are people who wanna make cool stuff and people who want it. It's a happy bunch.

On the other side, you got people (and companies) that want to use the Web to exploit others. From the small-time scammer to the multinational corporation, they simply want a bigger slice of the pie without giving anything in return.

For a while now, it seems we've been in a sort of balance. The average Joe Internet can buy stuff, find information, and share baby pictures easily and safely. All of that thanks to the indefatigable people building tools and educating users.

But this balance is threatened. A group of online advertisers, including Google, are mounting a new offensive. Their goal? To weave ads into the very fabric of the Internet: the web browser. Their weapon? A project called "Federated Learning of Cohorts."

What Is It?

Federated Learning of Cohorts - FLoC for short - is a new browser standard. It defines a feature that analyzes a user's browsing habits, distills it into a cohort (I will use the term "label" from now on), and exposes it to advertisers. With it, they can target ads more precisely and let go of the abomination that is the third party cookie.

At the time of writing (mid April, 2021), the feature is in the experimental stage. It has been rolled out to a small portion of Chrome users. The labeling algorithm, which runs once per week, is simple and limited to scanning visited domains. Similarly, the number of labels is limited to 256, which can only paint a fuzzy picture of the user.

The people behind FLoC have already expressed interest in swapping out the experimental algorithm for a more powerful one based on unsupervised machine learning. They would also increase the number of possible labels to tens of thousands. The last update would ensure cohort sizes of at most a few thousand users.

Why Does It Suck?

From a privacy perspective, the idea of getting labeled is awful. Imagine wearing a list of your preferences on your forehead, so that marketers can walk up to you, read it, and say, "I see you like hamburgers! Check out these Tasty-Snak burgers bla bla bla." It's creepy and undignified.

Limiting labels to only a few thousand users each makes it easier to identify unique users. Instead of being one amongst tens of millions of similar users, you would be one in a couple of thousand. And because browsing habits don't change quickly, it would be possible for advertisers to "follow" a user across labels.

But the bigger threat here is that FLoC would expose a wealth of behavioral data. It's every advertiser's, scammer's, and shady government's wet dream.

Just imagine how precise the labels must be if they group users by the couple-thousand. You'd have stuff like "people-who-like-anime-and-hot-dogs-and-read-literature-and-live-in-Memphis-and-are-between-18-and-24-years-old-and-browse-the-web-2-hours-a-day-and...."

It's already scary that targeted ads can figure out you're pregnant before you do. FLoC would make it even worse.

You think that's bad? Consider how this would expose any kind of minority traits. Don't limit yourself to just the ones we have in the U.S. Think globally! Imagine all the ethnic, sexual, and religious minorities. Add to that all of the supporters of opposition parties that live under repressive regimes. All of them would be instantly exposed by their own browser!

To this, Google has offered to act as a "benevolent" overseer. They offered to keep an eye on minority groups and intervene if FLoC would lead to their harm. But do we really want a corporation to act as global police? They don't have a good track record.

Where Does It Fit In the Bigger Picture?

FLoC, if it were accepted and rolled out, would codify advertising into the Net's DNA.

As a consequence, it would be more difficult to try out different ways of creating and sharing content online. It's a trap. We would essentially be stuck where we are today, with multi-megabyte ads auto-playing annoying music.

And what better way to cement your company's position than to make its product a core part of the Internet? Around 88 percent of Google's revenue comes from ads. (For Facebook, that's over 98 percent). If you already have enough power to push through technical standards FLoC, why not use that power to get more power?

I think that's what Google's and other advertisers' grand strategy is: literally become part of the Internet's infrastructure. Then, dismantling (anti-trust law) or replacing (competition) you is too costly and too risky.

What Now?

We've been here before. The Browser Wars of the early 00s taught us what to watch out for and how to fight back.

Already, groups like the Electronic Frontier Foundation are speaking up and educating people about the risks associated with FLoC. Other browser makers like Mozilla, Brave, DuckDuckGo, and even Apple have publicly expressed their opposition to the project. Even WordPress, which powers around a third of the Web's sites, has a proposal for blocking FLoC.

What can a regular person do? Apart from switching away from Chrome and supporting the EFF, I think education is the way to go.

Google and its gang are working hard to keep this quiet and to wrap it up in nice PR fluff. Can you believe they describe FLoC as "This API democratizes access to some information about an individual's general browsing history"? Well, in that light, I guess peeping Toms merely "democratize access" to individual's bodies. Disgusting.

So talk with your friends and family. Don't pressure - nobody likes a zealot. Explain to them what's going on, why it matters for you, and why it matters for them. Be ready to offer help too! Many people don't know how to install another browser or an ad-blocker.

Good luck!

Municipalities Pwned at Greater Rates!

by lg0p89

Municipalities have a very distinct problem. They are frequently targeted for ransomware and other attacks, as the attackers know their systems generally are not fully secure, unless they've been recently successfully attacked and have corrected and mitigated the issues. This is driven by budgetary constraints - not allowing the city, county, etc. to be able to hire the exceptional talent, purchase the tools needed in a timely manner, and other requisite uses for cybersecurity. While this is a Catch-22, it leaves these organizations in the wind, hoping to be obscure enough so that they are not noticed and attacked. Even a failed attack can have negative effects on the operations for many reasons.

One of these targeted was the city of Florence, located in Alabama. Florence, much like the city in Italy, sounds like an amazing place to live, located on the banks of the Tennessee River with many festivals and other attractions. This is not a massive metropolis, with nearly 40,000 residents. Of all the places to target, you have to wonder why Florence?

Attack

As you can guess, the city's computer system had been successfully attacked. The entry points were through the email system. Specifically, this was a phishing attack, and the unfortunate phishee was Steve Price, the IT manager. His credentials were acquired as part of the attack. The phishing email was one of the many samples of the DHL email, where there are dozens of email recipients, all receiving the same package with the same tracking number on the same day. These emails are pretty obvious as to what they really are intended for.

The illustrious and distinguished Brian Krebs notified the mayor's office of their system's compromise on May 26, 2020. From the published accounts, the city somehow did not know of the breach prior to this. This is odd, as seemingly someone in the IT department maybe should have noticed a strange IP address accessing the system and pulling data from the network. The following day, the system administrator did contact Mr. Krebs to let him know the computer and network account affected had been isolated and was not in service. It appeared the sysadmin did not quite understand the capabilities of the attackers

at this point. On June 5, 2020, the attackers finished deploying the ransomware and began their demand for the ransom payment. The city had 12 days to fully defend against the attack, however, unfortunately only did a part of the work required to address the issue.

When the city began to review the situation, it did not appear any of the affected system's data had been deleted or exfiltrated. This was probably a little too optimistic for the city.

On a side note, the attack occurred while the IT department was attempting to have the city council approve the expense for a third party to do a penetration test of the IT systems.

Ransom

The attackers were not going to work through the attack cycle for practice and mental gymnastics. The system has been operationalized into a business, and a rather profitable one measured by the return on investment (ROI). In this case the attackers were DoppelPaymer. They began the demand for ransom at $378,000 in bitcoin. The amount was negotiated down to $330,000 by a third-party firm, still in bitcoin. This does seem to be a rather large sum, given the size of the city. The attackers, however, have realized the power of their leverage on the systems.

Post-Attack

Once the city had the opportunity for a quick review, their IT department and a third-party, contracted by the city (Arete Advisors), began to adequately investigate the issue. As time had passed and more effort was placed into the investigation, the city realized the attackers may have at least a portion of the data on the affected systems. The city noted they just didn't know. One would presume they had sufficient access, such that if they wanted, they could have taken the data if they chose to. On this note, the investigation concluded the attackers had access beginning in early May 2020 and continuing for nearly the remainder of the month. During this time, the attackers had free access to roam about and check out the network. They borrowed without authorization the personal information on the city's employees and customers.

As they saw the writing on the wall, the city council voted unanimously to pay the ransom. The funds were to be paid from the insurance fund available for these types of issues.

A curious point with this is that the city required the attackers, DoppelPaymer, to provide proof they would delete the stolen information they had. The curiosity is, other than promising or a pinky-swear, there really wasn't a way to prove they would delete the data. This is one of the many problems with paying ransoms. The organization is depending on the attackers to follow through and not leave a backdoor or recurring malware on the system. Historically, the attackers have followed through and have not left any surprises behind for later easier attacks. They say there is honor among thieves, however, I would not bet on it. The city naturally is also working with law enforcement on the matter.

Afterthought

If you are management, the sysadmin, or on the cybersecurity team, please consider this occurrence or any of the thousands of other successful ransomware attacks as examples of why training and an adequate SIEM (security information and event management) are so important. While cybersecurity is the focus of the cybersecurity department or team, it is still everyone's job to be vigilant and not be click-happy. If they aren't expecting an email, don't know the person or organization it is from, or it simply leaves them wondering if the link or attachment is appropriate, don't do it. This will save so much time, energy, frustration, etc. for the staff and budget.

WRITERS NEEDED!

There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access,
our editorial department can be snail mailed at:
2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.

The Demise of Network Security

xcm@tuta.io

by XCM

Network security has had a fair share of relevance in the last 20 years or so. Traffic pattern types used to be few and predictable, software exposed on the Internet was relatively simple. So a stateful firewall for a long time was good enough of a safeguard.

Then things changed.

Software and attacks turned more complex and it became clear that blocking traffic on TCP ports associated with malware suddenly was not enough.

So antivirus and Intrusion Prevention Systems were bolted on top of stateful firewalls. Of course, these systems come with their limitations:

Traditional pattern-based antivirus solutions do not scale. On the wire, antivirus scanning can also be evaded by using different techniques such as packet fragmentation or by abusing specific protocol options or methods.

Pattern-based Intrusion Prevention Systems also do not scale, with the addition of acting on the assumption of what could happen on a given host based on what is observed on the wire, which is a pretty big assumption.

On top of that, encryption has become prevalent (finally and thankfully), so these security products must now perform a Man In The Middle attack on TLS encrypted sessions in order to gain visibility.

This is potentially bad as the end user does not have any way to verify which certificate is being presented by the server they are connecting to. Sure, they could trust the security device to verify it for them. Good luck!

Additionally, middle boxes might downgrade the encryption in order to increase compatibility.

This aside, decryption is clearly not the answer in the long run. Newer TLS versions might make things more complex for security vendors/criminals/government agencies.

Another problem is that when hosts use pinned certificates or mutual authentication, there is no known way to successfully decrypt, inspect and re-encrypt traffic.

What can we deduce from all this? Well, it seems to me that the days of network security could be doomed.

It might not happen tomorrow nor in five years' time, but network inspection devices will slowly lose the visibility they need to do their job.

Even with encryption aside for a moment, a traditional stateful firewall historically would allow host A to communicate with host B on TCP port 80, for instance.

So called Next Generation Firewalls might do the same, but while identifying the traffic as actual HTTP.

Still, do we really know who initiated the traffic and where it is going to?

Sort of. We know the IP address, the URL/FQDN or the user associated with that machine. All of these in the end translate to an IP address, not to a specific device.

Besides, can I verify that HTTP traffic was initiated by a browser under the control of the user? Nope. It could be from a shell spawned by a piece of malware running with some other privilege.

So what's the solution?

There are hosts of vendors who promise the panacea in the form of *"Traditional <insert technology here> do not work any longer. That's why at <insert vendor here> we offer unparalleled protection based on <insert buzz words here, such as machine learning / AI / magic>."*

The reality is that security is hard and the challenge increases exponentially if the attack is targeted.

In my opinion, a promising approach is somewhere towards total network abstraction.

Rather than focussing on decryption, URL filtering, firewalls, sandboxes, and the like, treat the network between host A and B as an untrusted, non-securable medium - regardless of network topology, distance between the endpoints, or "trust" level of the network equipment.

Reduce the security boundary to the only area where we still have a decent level of control: the endpoint.

A bit like in European medieval warfare where the keep was protected but the village outside the castle was not considered worth defending nor defendable.

So rather than trying to regulate protocols and applications on the wire, restrict them on the endpoint at a process level and for a specific user. So, for example, process X on host A can generate HTTP traffic (real HTTP, not data over TCP 80) towards process Y on host B, but only if these processes belong to determinate users.

Some security solutions already offer a similar level of micro-segmentation.

Additionally, instead of using IP addresses and hoping they corresponds to the hosts they should represent, we could use certificates.

A certificate exchange would be a strong way

to ensure the endpoints in the conversation are those we expect, assuming we trust the current certificate validation system.

As an additional measure, the initial TLS exchange could be used to negotiate an encrypted channel leveraging other technologies such as IPsec, OpenVPN, WireGuard, or others.

Even without antivirus, IPS, and sandboxes, having this kind of control could potentially limit the scope of successful attacks at various stages in the life cycle.

The level of visibility we get on a host under our "control," however, is not unparalleled. We still depend on closed source OSes, hypervisors, proprietary hardware, and a host of obscure firmwares with high privileges.

So what's the takeaway here?

There might not be an easy solution to the problem and probably there will never be, but I doubt that trying to pump new features in zombie technologies will bring us any closer to our goal.

The goal post shifts continually and, as my favorite author Edgar Allan Poe once said: "it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."

Whereas this has not been proven correct yet for most modern ciphers, it offers a glimpse on why the struggle between attackers and defenders is unlikely to end anytime soon.

In the last few years of the 1990s, around the time of a series of compulsive visits to the local bookstore (see my previous article in 37:2), I happened to purchase a volume on Visual Basic 6 out of boredom.

I convinced myself that it was about time I moved away from QBasic and its visual reincarnation made a decent fit. Or so I thought at the time.

I called one of my first tests with VB6 "Windows TD (Total Domination)." It was a parody of the installation process of a successful operating system.

While listening to the comforting music "borrowed" from the original OS, the user would be presented with a series of improbable splash screens enunciating the exciting new features they would soon benefit from.

I remember one of these boasting something along the lines of: "With Windows TD you do not have to worry about emails any longer. Windows will turn your PC on at night and independently interact with your recipients."

A couple of decades later, or a few weeks ago, I found myself composing a document using the editor endorsed by the company I work for. It is a web-based editor owned by an organization which also runs a very successful search engine.

This program helpfully employs autocompletion and it appears to be using a model that learns and adapts to the user's writing style. The more I wrote, the more the program would suggest words or ways to complete a phrase. The more I wrote, the more the model and I agreed on what should be written next.

I opened up the corporate chat service and joked that we are all unwittingly training a machine learning model which, one day, might completely do without us fragile humans.

Regardless of opinions on when/if the singularity will ever be reached, or whether we have already surpassed that milestone, one thing holds immediately true:

By training a machine learning (ML) model, I am indirectly cementing my biases. These might ultimately present themselves in any future write-ups of mine even when I would not have done so autonomously. Additionally, depending on how the algorithm is designed, my biases might ultimately spill out and influence other writers.

This conundrum is nothing new. There is an abundance of academic papers that highlight the reality of bias in machine learning models, even though these typically focus on bias intrinsic to the algorithm, rather than in the data.

The primary challenge is not just the fact in itself, as all humans are biased to begin with. Neither are all the privacy implications of an ML-powered text editor, important though they are.

What I find most concerning is the unexplored and unpredictable territory of a machine-evolved human bias.

After reading my post in the chat room, a colleague of mine was quick to point out: "Have you considered that while you believe it's predicting what you are thinking, it might be telling you what it wants you to write?"

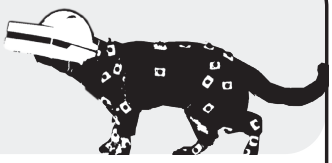
I must admit that until then I had foolishly thought I had been training the model, rather than entertaining the possibility of a premature inversion of roles.

I spent a few minutes pondering on a scenario I was not ready for.

Ultimately, denial and self-preservation kicked in. After stretching on my chair and gazing out of the window, I comforted myself that this was clearly just the product of a momentary lapse of reason.

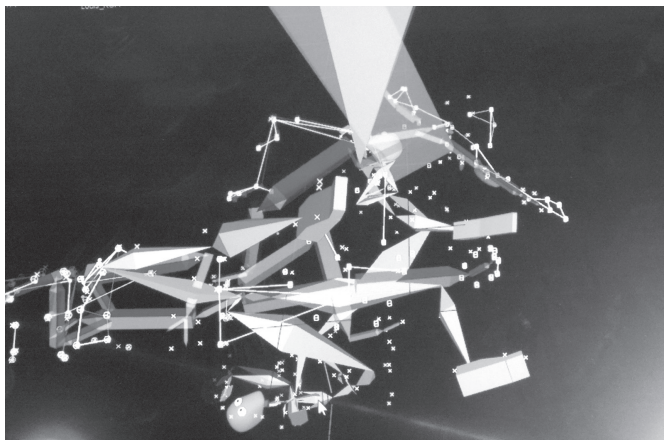
Exactly what I thought back in the 90s while joking about self-completing emails.

Hacking Motion Capture Software and Hardware



by Alan Sondheim

Hacking's most often associated with computers, social engineering, and so forth. There are many people working with glitch art as well as steganography, of course. For the past decade and a half I've been involved in hacking motion capture, in order to produce radically different BVH (Biovision Hierarchy Animation) files for animated avatars in virtual worlds, and in stand-alone videos made with Poser and other programs. In motion capture, sensors or reflectors are placed on the body of a performer; the output of the rigging is fed into a computer and transformed into a "behavioral model" paralleling the performer's movement. All well and good. But there are numerous ways to alter this and create amazing figures and movements almost beyond anything imaginable.

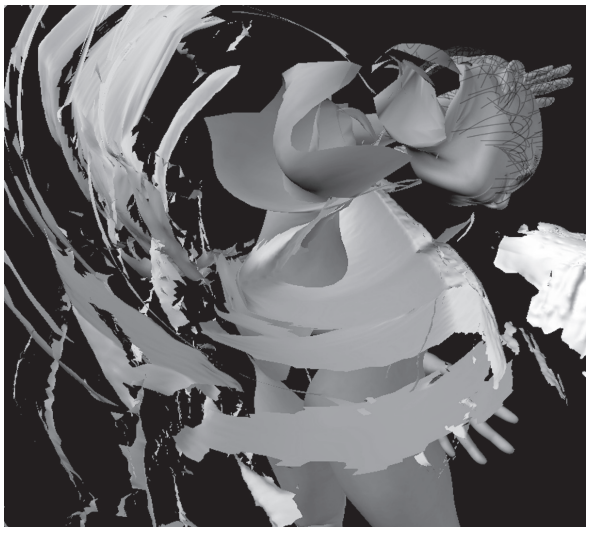


I began working in this direction years ago when I was given the opportunity for a residency in a virtual environments laboratory at West Virginia University in Morgantown. We found a disused motion capture setup that was quite old, even at the time; it worked through 18 sensors sending electromagnetic signals to an antenna that would locate them individually in space and time. The information was processed and output to an ASCII BVH file that could then form the basis for an animation.

We used this a couple of times and then began to experiment. I'm not a programmer, but I had an assistant who was, and I asked him to rewrite the interface itself. I thought that, just as there are various filters, for example, in Photoshop or Gimp that are mathematically defined, we might be able to create "behavioral filters" for mocap that would alter the output of the sensor mapping. My assistant located the mathematicals that governed the input-output chain and I noticed that most of the trigonometric functions were sines and cosines. Given the maverick behaviors of functions such as tangents or hyperbolic functions, we began substituting these in the equations. We were also able, of course, to change any governing constants. The results were amazing - avatar behaviors that were like nothing we had ever seen before. We basically had an interface that appeared to govern the representation of behaviors in new ways.

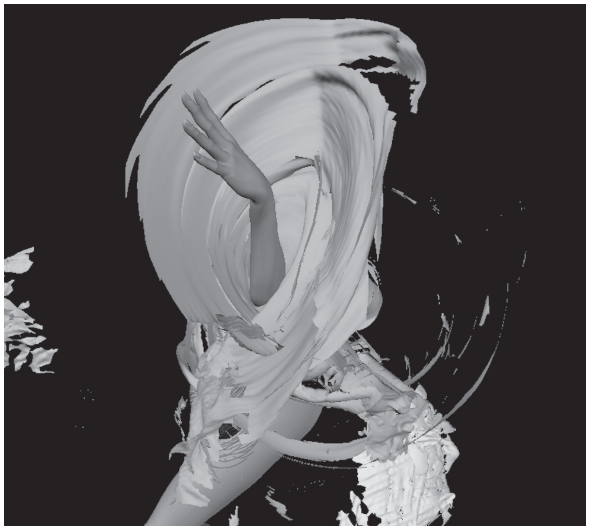
We didn't stop there; we also began working with the sensors themselves in order to create different body mappings altogether. This is something I've been exploring for years now at a number of different institutions. Random sensor placement is only of limited interest, but topological "smooth and/or broken" transformations work wonders. The remapping can be up and down, left to right, and so forth, but the sensors (on more complex mocap equipment with up to, say, 40 sensors) can be divided among several performers. If A wears the left-side sensors and B the right-hand ones, and then A and B separate, this "tears" the representation of the body; either the software breaks down, or the body appears to expand. If A and B rotate in opposite directions, the body "wraps" in layers; the trick is to stop the software input before breakdown. At one point we used trapezes in the studio, the sensors divided among four performers, and the results were incredible; at another point, we had the four performers

(student dancers) attempting to act coherently to create a single representation of a dancer that held together. The result was a dance created by the four performers themselves, in their constant adjustments to each other. (There were two



outputs: video of the human dancers, and video of the single avatar dancer; these were combined.)

The trick with all of these things is to produce a coherent output that can be used elsewhere. Some of the files were fed into Poser; some were fed directly into representations (say, of a bull); and the ones used in virtual worlds (OpenSim, MacGrid, and Second Life) produced amazing dances that seemed completely unworldly. There were two broad types of dances from the files: ones in which the body twisted itself into impossible shapes, and ones in which the



location of the body in the environment was also impossible - instantaneous changes of position, rotations, and so forth.

In all of these things (I've worked at a number of places by now on invitations to use a university's mocap studio), social engineering is critical; a lot of technicians would keep trying to "correct" the mocap or say it wouldn't function properly or at all, and, in return, I would keep insisting that in my work there was no proper functioning; we'd experiment and see what would happen. All of these other places, by the way, had sealed software, of course; it was only at WVU that we had the amazing luck to hack the software itself.

These explorations have had many interesting results - new ways of thinking about modeling the body, new ways of creating and translating dance choreographies for performance, and a wide variety of behaviors and avatars for gaming, etc. The most sophisticated approach is hacking the software itself (instead of, or in addition to, remapping the sensors directly). Since there are numerous mocap kits available, this should be somewhat simple. Modules could be organized like SuperCollider programs, inserted and removed when necessary. The results are immediate and almost always satisfying.

Examples

www.alansondheim.org/njitfriday
➥368.jpg
www.alansondheim.org/superherotet
➥hered1.png
www.alansondheim.org/vortex4.png
www.alansondheim.org/vortex2.png
www.alansondheim.org/singlemain.
➥mp4
www.youtube.com/watch?v=hZu-
➥FnwMc_U
www.youtube.com/watch?v=v2Z7
➥o1K3utg
www.youtube.com/watch?v=TNCL
➥XGInC1Y

How to Read *2600 Magazine*

by Delta Charlie
write2600@privacyphoenix.com

Receiving the Magazine

This article will benefit all readers of the print edition of *2600 Magazine*... no matter your skill level. My experience with *2600* is a 20-plus year relationship as a reader and multiple published writer (under various pseudonyms). There is an optimal way to read the physical copy of *2600* and I want to share with readers the experience of someone who has stacks and stacks of issues.

The first thing you want to do when your new copy comes in the mail is destroy the envelope it comes in. If you like keeping the envelopes, you may want to conceal the mailing address with a thick marker or a rolling security stamp. You know, one of those things that rolls random characters over a printed sheet of paper. If you destroy the envelope, a cross shredder is a good way to go. Maybe burn it and bury the ashes.

Back in the day, a common topic was how the three-letter agencies wanted to get their hands on the "*2600* list" of subscribers so they could put them on "watch" lists. Trust in *2600*. They've stated many times that their "master list" resides on a computer that doesn't even touch the Internet.

First Look

Find a safe location where you can relax for about 30 minutes to two hours, depending on how you like your first look of the new issue to be. Personally, I take about 30 minutes to get eyes on all the pieces that interest me. Then, time permitting, I take about another 30 minutes to actually read. My personal strategy requires me to spread my "quality time" with the magazine over three months. Sometimes I don't read, and just play around with the technical information in the articles. Sometimes I just read the letters and opinions, and don't touch the technical stuff. Just depends.

One important part of the first look is the physical handling of the magazine. *2600* has had a mostly staple-based binding. There was about a year where they tried a binding that was similar to a book (and hid a *surprise* message in the spine!), but eventually went back to staples. One problem that can occur is opening the magazine too fast. You'll risk the staples pushing against the fresh, thick cover paper, which may rip through and damage the magazine. What you want to do is physically and gently bend the magazine, and lay it flat gradually as the paper becomes more forgiving.

I personally used to enjoy going straight to page 33 (why did they stop that?) and trying to understand the cryptic messages. I vaguely remember only getting one of these solved - I think it was Morse code. (I left these to the much smarter readers to solve and maybe they will write about them in the letters.) The next thing I'd do is figure out the cover and the subliminal messages or watermarks. The pictures are always great in the magazine and I've had payphones published a few times; although a picture of a Hacker-Pschorr beer glass never got published. Relax the left side of your brain for a while and just enjoy the colors and pictures.

Reading

The next order of business is the editorial! Personally, I feel that the political and social commentary in this section is way too much. I read *2600* for the technical hacker information, with a secondary emphasis on hacker culture.

Next, we scan the index! Here's where I'll try to see if "EFFecting Digital Freedom" or "Telecom Informer" say something interesting, then scan if any other article catches my eye. I try to find anything New York City-related - like MetroCards were cool to read about for a while. I try to look for code snippets I can quickly throw into Python to play with, or just try to read to keep up on my minimal level of coding skills.

When I need to switch it up, I'll check on the letters or the marketplace. Personally, the marketplace and hacker conference listings are the areas that have served me the least, though if you're a traveler, this is an awesome resource. The hacker submissions have been a nice addition the last few years. I enjoy "The Naked Princess," but would much rather read it as a printed book... so hopefully that will happen.

Going Forward

Well... that's it for now. I don't think I've ever read an article about how to actually pick up and read this fine publication. I think it can spark some lively discussions in the letters sections about how everyone has their own *2600* "ritual." Thanks for a fine magazine!

P.S. This article was written entirely in Standard Notes and shared with the *2600* Secure Drop link, though I also submitted via the articles@2600.com email. Please keep privacy and security alive!

Verified Badges for Everyone?

by Corye Douglas

Note: This is an opinion piece that is sure to provoke discussion. We want to read your retorts and will print the best ones. articles@2600.com for long responses, letters@2600.com for short ones.

The threat of cybercrimes is growing - both in scope and intensity - as the government drags its feet on mandating cybersecurity policies to protect citizens. One fifth of U.S. Internet users who are minors report unwanted sexual solicitation, and half have faced cyberbullying via social media. Employment scams defraud job seekers by stealing personal information, financial data, or money. The FBI recently stated that possible abductors are luring children by posing to be in their age group and conceiving a relationship of false trust via social media platforms. It is evident that social media-based trafficking is on the rise during the coronavirus pandemic. The UN Committee on the Elimination of Discrimination against Women (CEDAW) now calls on social media platforms to help eliminate trafficking in women and girls, amid an increase in online traps designed to recruit potential victims during the COVID-19 pandemic.

The public's exposure to cybercrimes has increased in recent months as the COVID-19 pandemic has forced the world to shift to remote learning and employment. Many countries that were ill-prepared or unequipped to tackle cyberattacks now find themselves at increased risk. Children and adolescents are a primary target for these attacks. Since many schools now conduct classes online, kids are exposed to the Internet earlier and for longer durations than ever before. There is also a growing number of children using social media platforms, with or without their parents' knowledge and consent, under the age of 13.

Identifying, investigating, and punishing all occurrences of cybercrime is a tall order indeed. The cloak of anonymity granted by the Internet must be removed to reduce the time and effort required to locate culprits and charge them with cybercrimes. An innovative solution for accelerating this process is for social media platforms to require verification of all users when creating an account and for existing accounts to remain active. Current age verification protocols are easily overcome by children. No social media platform asks for any identification for adults, either. Even when malicious users are identified and their accounts disabled, without safeguards, a predator can easily switch to a new profile and search for another target.

Currently, it is difficult to locate unscrupulous web users, as anyone with an Internet-enabled device can log on and commit a crime without validating their identity. The FBI arrested only 1,200 identity thieves between 2003 and 2006, though nearly 8.3 million victims were reported during this time. Moreover, only a third of the arrests resulted in convictions. Many law enforcement authorities remain unaware of a majority of cyberbullying and sexual harassment instances due to underreporting. Vague jurisdiction laws and an inability to prosecute from a lack of concrete evidence further inhibit arrests and convictions. More identification and less anonymity are needed to bring cybercriminals to justice.

Social media specifically is linked to many more forms of cybercrime: stalking, hacking personal accounts to steal identities, impersonating someone else to gain confidence of victims, and more. There are even instances of vacation robberies: a predator clues in to Facebook pictures and posts not only to recognize when targets are on holiday but also to identify their addresses and potential whereabouts. An entire TV series is devoted to unveiling those who are "catfishing" - romantically wooing victims online under false pretenses over a period of time, often stealing money from their victims. Instances abound of shared links that promise freebies, only to divert the user to a malicious website. In fact, the dark net is now reaching out to social media accounts to sell and share tools for developing hacking skills.

One way to eliminate user anonymity while preserving privacy is linking the social media platforms and the State Department of Motor Vehicles or Motor Vehicle Commission through auto-redirect verification; PayPal and ecommerce websites employ this strategy in a similar fashion. This process will use public and private keys to encrypt the transaction from the social media platform to the DMV or MVC website. The encryption will hide the user's PII and it would not be visible to anyone viewing the website

source code. Social media platforms would not store or have access to any identifying data on their servers, limiting the scope of damage in the case of a data breach.

Requiring verification of all user accounts will ensure a decrease in the incidence of criminal activity. Consider, for example, the case of prepaid and post-paid mobile accounts involved in criminal activities and terrorist attacks. Although burner phones are still used in some crimes, the added security feature of a required ID check for phone purchases provides ongoing mitigation. Identity verification acts as a powerful deterrent for most offenders.

Government cybersecurity guidelines would be an advantage for social media platforms in ensuring complete and consistent safety and privacy of all user verification. However, considering the fragmented nature of cybersecurity regulations in the U.S. at present, the possibility of arriving at universal protocols for sharing, storing, and "forgetting" personal information is distant.

The call for accountability on social media platforms has become a strong demand to protect vulnerable groups accelerated by the shift to more online exchanges during the COVID-19 pandemic. With cybersecurity policy always lagging behind cybercriminals' creativity, early adoption of a proactive solution, such as 100 percent ID verification as a mandatory requirement for social media account holders, is an essential step toward mitigating cybercrimes, as well as meeting the UN call to mitigate online risks of exposing women and girls to trafficking and sexual exploitation.

Gone Fishin'

by dcole

Recently, I decided to start learning some server-side programming for a project that I had in mind. Having used JavaScript on the client side in the past, I choose node.js as my server-side runtime due to my familiarity with the aforementioned language. If you are not familiar with node.js, it is simply a JavaScript runtime built on Chrome's V8 JavaScript engine that runs on the command line of pretty much any operating system. My project was to consist of a web page where people could post a message. This message would then be sent using a client-side script to a web facing CouchDB server. Node.js was used at this point solely to serve the web page itself.

While starting the project, I initially wrote a short server-side test script that would respond to incoming requests from the web and display what those requests were on the console. After testing the script on my local network, I opened up a port on the router. This allowed me to test the server from outside my local network which was successful. As it was late in the evening at this point, I failed to remember to exit my server process and close the port on the router before heading to bed.

The next evening after work when I got back to programming, I found various requests on the terminal that I did not ask of my server. Noticing I left my router port open to the wild, it dawned on me that these requests were made from the outside world. This must be all those malicious hackers and script kiddies I hear of trying to gain access to my server to wreak havoc! Being a naturally curious fellow, this situation gave me the brilliant idea of going fishing for requests, basically setting up a honey pot. For my fishing lure, I used the following code saved as fishing.js:

```
const http = require('http');
const requestIp =
➥require('request-ip');

http.createServer((req, res) => {
  req.on('data', () => {})
  req.on('end', () => {
    const ip = requestIp.
➥getClientIp(req);
    console.log(`\u001b[34m${ip}\
➥u001b[0m: \u001b[32m${req.
➥method}\u001b[0m ${req.url}`);
    res.statusCode = 404;
    res.end();
  })
  req.on('error', e => {console.
➥error(e);})
}).listen(8080);
```

The above code accepts an incoming request, pleasantly displaying it on the console and responds to the request with a 404 (Not Found)

code. I then ran this code for approximately three days using the following commands in a Bash shell on my server:

```
node fishing.js > fishing.log &
disown
```

Asking the server process to run in the background with the "&" symbol and running the command "disown" after allowed me to end my SSH session with my server while keeping the fishing program running. After the three days were over, I logged back into my server and ran the following commands to terminate the process:

```
ps -aux | grep node
kill pid
```

After killing my node process, I opened up the fishing.log file and proceeded to extract some interesting information. I received 192 requests in total during the three days I let this fishing lure run. Out of these total requests, 174 were GET requests. In total, 114 unique IPs made requests with one IP having sent 36 requests. The majority of IPs sent between one and nine requests though. The most requested URL was "/" or a root request. The next most requested URLs were as follows:

```
/currentsetting.htm
/vendor/phpunit/phpunit/src/
➥Util/PHP/eval-stdin.php
/?a=fetch&content=<php>die(@
➥md5(HelloThinkCMF))</php>
/?XDEBUG_SESSION_
➥START=phpstorm
```

Now, I understand this information is nothing new to administrators of web servers, but this was new to me. These types of requests have shown up in request logs for decades now. I gather the requested URLs change over time as new vulnerabilities are found as well. Having attempted a little Internet research, I was able to find out "/currentsetting.htm" is likely a Netgear router exploit and the other three mentioned requests above are all PHP exploits (though I didn't need the Internet to tell me that since PHP is right in the request!).

The initial shock of seeing these requests was quickly overcome by the knowledge that most of these requests are aiming at fairly specific exploits. If you are not running PHP, no worries. If you don't have a Netgear router, no worries. Being aware of these attacks can allow one to be on guard and keep tabs on the latest potential vulnerabilities.

What did I learn from this situation? I learned that it is important to pay attention to how you plan your web facing programs. Initially, I was programming my web server without security in mind due to lack of experience with this type of programming. My CouchDB server was open to the wild and my web server had no filtering for incoming requests. After the experience of finding these requests accidentally, I changed my methods and started programming with security in mind. I moved my CouchDB behind the web server code and started filtering for valid requests and denying the rest. The client-side script would now send the posted messages to the server and the server handled posting the messages to the CouchDB. Initially, with the CouchDB server open to the wild, anyone and their dog with some "curl" skills could have deleted all my databases or injected a bunch of useless information into them. This would have been a kick to the nuts if I had gone live with the initial setup.

What I hope other people who are new to web programming take away from this article is that your initial ideas and excitement may lead you to program in a way that leaves your data or servers vulnerable to exploits. Take some time at the beginning for a little research and think of your project as a whole in terms of its security needs and vulnerabilities. This may help reduce the number of iterations required to produce a project as well as reduce the potential failure points. Have fun and code on!

The Hacker Perspective

by Cintaks Airer

My pre-hacker years probably began in the 1970s when I built electronics projects from Radio Shack kits. I built a number of radios, blinking lights, amplifiers, and noisemakers using the spring-clip wiring that made building and tearing down projects simple.

It wasn't until I had discovered personal computers that I think I truly began to feel the hacker spirit. Home computers were not nearly as common in the late 1970s as they are now. I remember the Radio Shack salesmen at the local mall patiently watching as kids came in and typed away on their display machine. I took a formal independent study class in BASIC in junior high school. I began buying books and magazines that specialized in computers and programming. I also watched the television series *Computer Chronicles* on PBS regularly in the 1980s.

My parents bought me a used TRS-80 that came with a number of books and programs on cassette. After getting bored with the game *Temple of Apshai - Dunjonquest*, I found the area in memory where the player's strength and stamina attributes were kept. Between the two-part loading process of the game, I added some code to POKE all high values into those attributes... bigger than the game was supposed to handle. The monsters and other enemies the player would face then posed no harm. I used my invulnerable player to then start mapping out the various areas of the dungeons.

I soon learned Z-80 assembly language. I used this low-level coding power to do all sorts of things with my TRS-80. I simulated some auto-start game features for one of Big Five Software's games. I made a burglar alarm that reacted to noise using the cassette input ports and an input amplifier. I used various tools to tinker with some games that I had, giving me more player lives in some of them and such.

In high school, I had access to Apple II computers. I used these to teach myself 6502 assembly language. I began by hand-assembling my code. I entered the code into memory in hex using the "CALL -151" monitor. Later, I found out how to invoke the mini-assembler.

I was asked to see if I could "fix" a program that the school faculty had purchased. They had bought a BASIC program that managed large-group competitions of a specific kind. Our school was the host for a competition that year, so they bought this software to help arrange the competition schedules and to print out the room-level schedules. Unfortunately, the program was only able to handle a small number of schools. The faculty had needed it to handle more schools. My job was to make that happen.

I found the IF statement in the code that limited the number of participants. I removed that which was all that needed to happen. I then spent the rest of my time doing data entry for the different school data. All went well with the actual competition. I was paid for my time at minimum wage. I made a whopping 12 dollars for my efforts. This was the first sum of money I'd ever made using a computer. I suspect that there were other versions of the software from the vendor which could have handled the larger number of schools.

I bought a Commodore 64 and 1541 disk drive. One of the first programs I typed in from a hex listing was Bill Yee's *Micromon 64*. It was a machine language "monitor" program that allowed scrollable viewing of memory in hex and scrollable disassembly of memory. One could also change memory and enter 6502/6510 instructions directly.

I soon bought a 300 baud modem. In 1984, I called a local BBS that I had found from an ad. This BBS had a listing of other BBSes. I was hooked. Most of the users of the local BBS scene used handles instead of their real names on these systems. When presented with the new user sign-up screen on a BBS, I quickly came up with the name "Cintaks Airer" - a play on the "Syntax Error?" message that many BASIC coders ran into.

I soon ran into many in my area who were also Commodore 64 enthusiasts. I found it pleasant that other assembly language coders could be found in the local area. Many of the patrons of certain BBSes were interested in removing the copy protection from games.

I only removed one scheme from a Commodore 64 game that used an error check on an intentionally damaged track on the disk. The code was easy to find and NOP out. There were many around who were much better at that sort of thing.

I became acquainted with a local hacker who was mildly into phone hacking. He used to conference with other hackers using a phone number that constantly issued a busy signal. The group found that they could all speak over the busy signal, having nightly conference calls.

I had a lot more fun playing with the BBS systems themselves. The terminal program that had been supplied with my modem only had bare functionality. When line noise caused the terminal to spit out characters that changed the text color, I decided to figure out how terminal software worked. I wrote my own that ANDed all input bytes with 0x7f, limiting the characters my terminal displayed to strict ASCII and not the extended color-changing characters in my computer's PETSCII encoding.

I also found out that I could change the two characters used as the baud rate divisor when I opened the channel to the modem in my code so that I could choose from a variety of non-standard baud rates. A local CP/M-based BBS honored both 400 and 450 baud, so I tried those with my own terminal software. While those worked for the most part, they were prone to a fair amount of "garbage" characters showing up, likely due to the limits of the software-emulated UART used by the Commodore 64.

I found myself on a new BBS using software I'd never heard of. According to the description, it was written in BASIC with some machine code for the time-critical functions.

I went to the download section and tried to download files with wildcard characters and I/O modifiers in the names. When I typed in "T*,S,R", I got the first file with the letter "T" that was of type SEQ (sequential) opened in read-only mode. By going through several letters, I found the file that was the introductory text file that each user saw just before being presented with the login prompt.

After downloading that file, I edited it to add "** Cintaks Airer was here **" after the initial greeting. I then uploaded the file using the wildcarded filename in addition to the ",S,W" modifier (SEQuential / Write). This overwrote the BBS greeting file. When I logged in again, there was my handle, neatly centered in the rest of the text. I left feedback to the Sysop, Matt, to let him know what I'd done and what he needed to look at in his code to prevent that from happening.

Matt was intrigued by what I had done. He thanked me for not doing something destructive. I helped him to find the areas of the download section that he needed to fix. He did the heavy lifting himself. I ended up writing a "chat with Sysop" subroutine in assembly language that he incorporated into the board. I suppose that this may have been my first contribution to open source, although I don't think Matt's modifications were passed around to more than a few folks.

I found out that pulse-dialing was accomplished by hanging-up then re-engaging the phone line in punctuated bursts. I added this functionality to my terminal program. Mine pulse-dialed more quickly than the pulse-dialers in some other terminal programs.

I later got a 1200 baud "dumb" modem that had tone-dial capability. It did not respect the Hayes "AT" command set. I had to disassemble the terminal that came with it to find out how to get it to tone-dial. This feature was soon added to my custom terminal.

In April of 1986, I was watching the movie *The Falcon and the Snowman* as it aired on HBO. The transmission was taken over by an individual going by the name "Captain Midnight" who interrupted HBO's transmission for many HBO subscribers. I asked on a BBS if this was some new hacker fad. I was quickly schooled on the term "hacker" by a bunch of local techies including a doctor who liked to churn out Z-80 code. I believe that this was the first time I had heard the definition of the word "hacker" portrayed in a positive light as someone who likes to explore technologies. In a short while, I had found my way to Steven Levy's book *Hackers,* which solidified the proper meaning of the term for me.

I bought a Commodore 128 as soon as they hit the shelves. I used the CP/M mode frequently. We had a strong local CP/M community complete with a couple of BBSes and a wealth of downloadable software. Most of this software was provided with source code and binaries, although the term "open source" had not yet been used. This was just the way most of these folks packaged up software. CP/M permitted me to run Turbo Pascal, which was way ahead of the competition.

A local BBS began to carry FIDONet echo conferences, which permitted me to converse with people all over the U.S. and the world.

I had gotten a job first programming on a mainframe and then on distributed MS-DOS computers. The DOS programming was in C and assembly language. I ended up buying my own MS-DOS machine. I dug deeply into the OS and hardware. I used direct video access in the EGA and VGA graphics hardware. I wrote TSRs and device drivers, although most of my device drivers were just TSRs that a client wanted to load up in the CONFIG.SYS so that no one could unload them.

I was asked to perform a security test on a commercial security system for MS-DOS. I was

given a PC with a word processor document in a "protected" directory. I had access to the DOS DEBUG utility, so I disassembled the code for the INT 21h vector. I found the code that did a security check before major operations and I NOP'ed it out. I then was able to read the file. The company had said that they had several thousand installations and that no one had ever done this. For a while, they were worried that I was going to publish details of the circumvention, but I hadn't (until now).

I then learned Windows API-level programming. The Windows API still serves me well. I wrote a program years ago that iterates through all visible windows and forcibly enables all child windows. This enables grayed-out buttons, drop-downs, and data entry fields. Most programs should know whether a control is disabled without knowing its state, but no one seems to follow that practice. Enabling these controls in some applications (which includes some current Windows system applications) permits you to tinker with areas of the program that are supposed to be off limits in certain circumstances.

I sold software using the "shareware" model for a number of years. I soon found that I had to apply copy protection to my own programs. I developed a few techniques that thwarted some attempts to use my software without paying for it. Some techniques worked well, some didn't. I found that some of the tricks I was using in my code triggered warnings in anti-malware software. I spent a fair amount of time submitting new releases of my code to the anti-malware vendors after the code was marked as "suspicious."

I used to get payments from all over the world through snail mail. I had a collection of physical mail from a lot of places for a long while. I was impressed that my little niche software was being used all over the globe and in large tech companies.

My local bookstore began carrying a magazine called *2600*, which I had heard of. Once I picked up an issue in 1994, I was hooked. I've never missed an issue since.

My foray into the world of the Internet came at around this time. I had heard of the Internet when the "Morris Worm" made the news in the late 1980s. A coworker tried to explain the fingerd exploit to me, but I was still clueless as to how this all worked.

I had been using CompuServe as a paid online service that permitted me to have an Internet email address. Some time around 1994, they offered dial-up Internet access using the Point-to-Point Protocol (PPP). You logged into CompuServe normally, then issued the command GO PPP. Then, you fired up Trumpet Winsock to provide a TCP stack that permitted TCP access through the service.

I began viewing these new-to-me websites using Spry Mosaic as the browser. I picked up a book on HTML. I got a shell account with a newly formed Internet Service Provider and I stood up my first web page. I learned how to write Perl and C Common Gateway Interface (CGI) code from the NCSA web server documentation.

I liked working on Internet code so much that I left my job for employment as an Internet coding consultant. I wrote a few CGI programs for clients and I taught a few HTML classes. I was already teaching programming classes at my alma mater tech school. I soon began to teach HTML and web programming there.

In the mid 1990s, I had published what I believe to be one of the first web (CGI) programming articles in print in a special edition of *Dr. Dobbs Journal*.

My technical pastimes have continued over these last 25 years.

Over time, my personal definition of "hacker" has come to mean someone who acquires technical intimacy with a system or systems by amassing enough knowledge to exploit previously untapped potential of said systems.

Cintaks Airer remains engaged in a career in the financial computing industry. He likes to tinker with a variety of programming languages. While he uses Rust, Go, and other modern niceties, he's looking forward to writing his first lines of 6809 assembly code soon.

HACKER PERSPECTIVE
submissions have closed again.

We will be opening them again in the future so write your submission now and have it ready to send!

Vulnerabilities in Deep Artificial Neural Networks

by Thor Mirchandani

0. Motivation

It should be no big revelation that artificial intelligence (AI) has become an essential part of life in a modern society, to the point that we take it for granted and assume that it's something that simply works. The reality is that artifical intelligence today, in all except its most advanced and specialized guises, is not all that intelligent. In general, AI is vastly inferior to "natural stupidity" of the form often encountered in humans and other organic life forms. (The main exceptions to that statement are the classes of systems that routinely beat humans at Go, chess, and other games.) Thus it's fairly safe to assume that whenever you encounter an AI system, on some level or in some way it is dumber than a bag of hammers, and, as everyone knows, where there's stupidity there is vulnerability.

This article is focusing on a particular type of vulnerability that is found in many AI systems implemented using artificial neural networks. The goal is to raise the awareness of the existence of this type of vulnerability and to show how relatively easy they are to exploit, while not providing a recipe for actually exploiting them. Therefore we will only present a blueprint for a general methodology, and not provide details of specific attacks.

1. Demystifying Artificial Neural Networks

An artificial neural network is organized in multiple layers of artificial neurons. Each neuron has one or more inputs and a single output. The outputs of neurons of lower layers are connected to the inputs of the neurons in higher layers. Only a fraction of the output signals are passed on to the higher layers, and the size of this fraction is determined by multipliers called weights. The weights are trainable, and it is this property that gives artificial neural networks their power. There are many well-known and efficient training algorithms. One of the most common and easiest to understand is supervised training. Here we present the input with some form of data, and let the network "guess" what type of data it is. If the answer is correct, we strengthen the weights associated with the input and the guess. If it was incorrect, we weaken the strength of the weights that were involved in the bad decision. If all goes well, the network gets better and better at inferring the correct output from the inputs until it achieves mastery, and we say it is trained.

We should distinguish between the output and inputs of the neurons and the outputs and inputs of the network as a whole. A neuron always has a single output, whereas the network can have more than one. The distinction will be important to the example that follows in Section 3.

The specifics of how the neurons, layers, and weights are organized determines the functionality of the network and is beyond the scope of this article. Instead, we point the interested to Aurelien Geron's book *Hands-on Machine Learning with Scikit-Learn, Keras and Tensorflow* for an excellent detailed introduction. We also recommend the book *Deep Learning Illustrated* by Jon Krohn for a more gentle starting point.

2. AI on Edge Devices

The training of a network is typically a very resource-intensive, one-time process. For that reason, it is often done using clusters of rented high-performance hardware in the cloud.

On the other hand, once a network is trained, it doesn't take nearly as many computing resources to operate it. In fact, many networks can run comfortably on single-board systems, such as Raspberry Pi, or even on micro-controllers, for example, some newer Arduino variants. The result is that AI has become ubiquitous on edge devices.

Since such edge devices usually don't have the computing power necessary for doing training, the weights of the networks inside them are fixed and no longer trainable. The network's run-time configuration is static. This is part of the basis for the type of vulnerability we're discussing.

3. Distilling the Essence of Catness

Let's illustrate the vulnerability with a simple example involving the Internet's favorite felines. Alice has trained an artificial neural network to recognize cats in images. The network can successfully recognize cats regardless of color, size, posture, or position in the images. It even recognizes partial cats.

The input to the network consists of the pixels in an individual image. The output is a single value ranging from zero percent to 100 percent, indicating how convinced the network is that a cat is present in an image. Zero percent means no cat, 100 percent means that the network believes there's definitely a cat in the image.

Alice shows the network to Bob and lets him play around with it. After a while, Bob gets bored. He asks himself "I wonder what would happen if I run the network backwards, using the output as a single input, and the inputs as multiple network outputs?" Thought turns into action, and he reconfigures the network accordingly. This is easy to do, since the network is purely software and he can simply copy the code for the weights and write his own reverse network code around that. (The weights are typically implemented as matrices of floating point numbers, and to the software there's nothing special about the weights that makes them different from

any other matrix from a computation standpoint.)

Once he's modified the network code, he applies the value 100 percent to the former output, which is now the input. That value is passed through the network's weights and some values appear on the outputs, formerly known as inputs. Bob realizes that he could use those values as the pixels in an image.

An image produced in that way has some interesting properties. First, it doesn't look anything like a cat. Since it was derived from the value 100 percent cat, it can be thought of as a simultaneous image of every possible cat, whole or partial, that the network is capable of recognizing. To the human eye, and to other neural networks that are not similar to Alice's, it looks like colorful random noise.

Second, if you present that image to Alice's network, it will be recognized as 100 percent cat. That's not surprising. The interesting part is that some such images have the property that when the image or part of it appears inside another image, that image will be recognized as 100 percent cat irrespective of what it really is an image of. (A famous example of this phenomenon is the "Psychedelic Toaster," a sticker made by Google in 2018. If that sticker is placed on an object in an image, that image will be recognized as an image of a toaster, no matter what it actually depicts.)

Naturally, Alice is incensed by Bob's little experiment. She decides to thwart him by burning the trained network into read-only memory inside an embedded system. That way Bob can't reconfigure the network to run backwards. She has now created an AI edge device capable of reliably detecting cats and nothing else. Satisfied, she starts to market it to people who are allergic to cats and makes a pretty penny.

Bob is stumped, since he no longer has access to the weights or the network code. It's a black box, sealed with epoxy. Therefore he cannot create the inverse network and distill its 100 percent catness. Problem solved!

4. Not So Fast, Alice...

As it turns out, Bob doesn't need the weights or the source code to create a distilled essence of catness image. The box is not black after all. Bob can use AI in the form of artificial neural networks to make the box transparent.

One naive way to peek inside the box would be to feed random data to Alice's network, hoping to stumble on a combination that will show the output 100 percent cat. That's a simple and great way to do it - if you have a very long life expectancy. Bob decides to work smarter than that. After all, the cat images are high resolution and have 24-bit color depth. Good luck stumbling on the right combination before the sun goes supernova!

Bob's first step is to create and train his own cat detection network. He takes great pains to ensure that the network is not identical to Alice's network. For example, the number of layers, neurons, or values of the weights could be different. In practice, even an identical network that is trained with a different set of cat images might do the trick as well, but Bob wants to be sure so he cooks up his own design that's not based on Alice's. The only parameter that is the same is the number of inputs. He calls this network The Critic. He trains it to reliably detect cats.

Bob's next step is to create a second network that he calls The Generator. The number of outputs is the same as the number of inputs of The Critic and of Alice's network. This is so the output can be used as an "image" by those networks. He doesn't train this network.

Then Bob buys one of Alice's AI edge devices from an unsuspecting online dealer. He's now ready to go.

Bob hooks the networks together so that The Generator's "image" output is simultaneously fed to the inputs of The Critic and Alice's device. The outputs of The Critic and Alice's device are used as the training goal, that is to decide if The Generator has created an image that looks like a cat to Alice's network and, at the same time, doesn't look like a cat to The Critic. The last part is critical. After all, Bob's goal is not to generate a bunch of deep-fake cat images!

The first images generated by The Generator are pure gobbledygook, that both The Critic and Alice's network classify as zero percent cat. Since zero percent and zero percent is not the goal, the weights are adjusted using one of the well-known algorithms, and he runs it again, and again. Before breakfast the next day, he sees the magic numbers zero percent from The Critic and 100 percent from Alice's network. In other words, Alice's network thinks it's a cat, but The Critic says "there's no way that blob is a kitty." He now has created a distilled essence of catness image.

Here's the twist: He actually has done far more than that. He now has a fully trained network, The Generator that, when run all by itself, can reliably create any number of distilled essence of catness images. We leave it as an exercise for the reader to think about scenarios where that can be useful. And what's more, Bob built his Generator network without knowing anything beyond the input and output formats of Alice's device. Great work, Bob!

5. Conclusion

The example above demonstrates, at a very high level, how to exploit a vulnerability that is present in many types of artificial neural networks found in AI edge devices. Obviously, we made many gross simplifications, and all the details were glossed over. The goal was to demonstrate the general principles of the vulnerability and the methodology underlying the exploit without getting into specific implementation details. In practice, the detail specifics are dictated by the type and

configuration of the network present in the device of interest, and Generators and Critics have to be carefully designed and trained accordingly. That process is the topic of another article.

Clearly this vulnerability is not limited to cats or even to images. In general, networks' architectures often used for classification and detection can be vulnerable. (For example, our hypothetical friend Bob has subsequently distilled the essence of dog and hamster....)

Opportunities for malfeasance abound: The Hamburglar might create a sticker that makes the license plate of his car indistinguishable from that of the police chief's car, and use another cleverly designed sticker to give himself a solid digital alibi. The call of the ivory-billed woodpecker heard in Alaska might shock ornithologists and void its endangered status. Swat teams could turn into crooks and crooks into swat teams.

All of those things would be very bad, and we condemn and discourage them in the strongest terms. But what if we look at it in a slightly different way, and, instead of labeling the phenomenon a vulnerability that may be exploited, we simply call it a behavior innate to certain types of systems? Let's face it, it is both well known and well documented that every sufficiently stupid system is ridden with unexpected behaviors, whether you prefer to call them features, bugs, vulnerabilities, zero days, design limitations, or something else entirely. For those of us who are not Hamburglars or crooks, unexpected behaviors present opportunities for new discoveries and warrant further study.

Is it possible that the behavior described above could be used for something good? Consider the situation when you have an essence of cat image. To what extent and in what ways would one have to modify that image to make it no longer be an essence of cat image?

A conclusive answer to that simple question could pave ways for novel methods for anomaly detection, including quality control, security, or even medical diagnostics. Other proposed applications are error correction, stealth technology, uncloaking stealth technology, finding interesting portions in text or genomes, building digital invisibility cloaks, and de-noising noisy signals just to name a few, all things that could serve us in beneficial ways. The answers to other questions may yield avenues to even more fascinating and useful discoveries.

On the other extreme, it's easy to imagine two warring AIs using technologies related to Bob's to battle each other, and the winner of the contest eventually turning humankind into AA-batteries. Technology is neither good nor evil, it's how we choose to use it that determines the outcome. Choose well.

Shouts to John, Kirk, Joao, and Saravanan.

The Telegraph Regulations and Email

by Cheshire Catalyst

Cheshire@2600.Com

What is a Telegram? According to the Merriam-Webster Dictionary (www.➥merriam-webster.com/dictionary/➥telegram), a telegram is "a telegraphic dispatch."

Telegrams are meant to be "dispatched" by electrical or electronic means. Morse code is electrical in nature since it is represented by simple on and off switches of electrical current, symbolized by dots for short on periods, and dashes for longer periods of the telegraph key being held down.

Emile Baudot of France took this simple means of telegraphic transmission and converted it to a code that could be sent via a typewriter-like keyboard, called the Baudot code, and telex was born.

What is telex? According to the Merriam-Webster.com Dictionary (www.merriam-➥webster.com/dictionary/telex), telex is "a communication service involving teletypewriters connected by wire through automatic exchanges."

As a "phone phreak," I found the ITU (International Telecommunication Union) early, and found that many of the Bell System Practices that made up American telephone service were translated into the "recommendations" of the ITU. As an international standards body, the ITU cannot require anything of a sovereign government. While phones are operated by "recognized private operating agencies" like AT&T in the United States and Bell Canada in Canada, they are run by government-operated post offices in many other countries. So the ITU can only make "recommendations" to those governments, which are what the ITU standards are called, yet tend to have the force of law in most countries.

As I became more interested in the data circuits of the telephone network, I found myself in the realm of the Telegraph Regulations, since the ones and zeroes of the data world were translations of the dits and dahs of the Morse code world of the telegraph. It was how the world transitioned into data from "what they already had," and old Emile was there waiting for them with his Baudot code working the telex circuits. So while Baudot was institutionalized as ITA2 (International Telegraph Alphabet Number Two), ASCII, the American Standard Code for Information Interchange, was established at ITA5 (ITA3 and ITA4 were forward error correcting (FEC) versions of Baudot for radio transmission).

By the way, the equals sign (=) character) in Morse code is made up of the run together letters B −... T − (−...−), and is used to mean "break text" between paragraphs in long telex messages, and also between the text of a telegram and the signature of the sender. The Telegraph Regulations state: "The signature shall be indented five or more spaces," which is why I indent my signature in emails, though the software many times removes excess spaces. I consider emails, and even SMS text messages, to be the direct linear descendant of telegrams. When I "sign" SMS messages, I use an "=" character before my "signature."

(This is how I send a text = Cheshire)

In my email messages, I use two "new line" (line feed) characters between the last line of my message and the start of my "signature tag." Again, the ITU Telegraph Regulations state that in a telegram, "the signature shall be indented five or more spaces," and for those of us who follow Internet regulations, we know the difference between *may* and *shall*. ("May" means optional, and "shall" means must!) Some email systems take multiple spaces as wasted space, and deletes most of it, so I use a sequence of <space><dot><space> and then another eight spaces, so that my signature gets indented a bit, if not completely to ITU standards.

Richard Cheshire is known in phreak and hacker circles as The Cheshire Catalyst, a pseudonym he's used since publishing in the TAP *newsletter of the 1970s and 1980s. He is currently retired, and is a volunteer at space museums near the Canaveral Spaceport, and hosts rocket launch viewings at Space View Park in Titusvile Florida. You are invited to join him for a launch any time (SpaceViewPark.Com).*

Facebook and the FBI

3:35 AM (10 hours ago)

Records
<records@records.facebook.com>

Hello,

This notice is to inform you that we received legal process from law enforcement seeking information about your account, and produced data as required by law. The legal process was accompanied by an order that prohibited us from disclosing information about the case until a specific time had expired and we were legally required to produce the records specified in the demand.

If you would like additional information about the legal process, please let us know as soon as possible by responding to this email.

Thank you,
Law Enforcement Response Team

This little surprise was emailed to us earlier this year (in the middle of the night) concerning one of our Facebook accounts that's hardly ever used. It certainly piqued our interest, so we accepted their offer to find out more. Six minutes later, we received the following:

2:17 PM (3 minutes ago)

Records
<records@records.facebook.com>

Hello,

For more information, the requesting agency may be reached at the contact information below.

Agency contact information: United States Federal Bureau of Investigation
Agency case number: 19MAG11541 or 2017R00439
Court: United States District Court, Southern District of New York

We are unable to provide you with legal advice. If you have questions about this notification, we suggest that you consult with an attorney.

Thank you,
Law Enforcement Response Team

NOTICE: This email (including any attachments) may contain information that is private, confidential, or protected by attorney-client or other privilege. Unless you are the intended recipient, you may not use, copy, or retransmit the email or its contents.

For information please visit: https://www.facebook.com/safety/groups/law/guidelines/ and http://help.instagram.com/494561080557017/

So basically, all Facebook could do was point the finger at the FBI. We contacted the FBI repeatedly to find out what this was all about, but they refuse to say a word. We were able to social engineer the name of the agent involved and discovered that he works in counter-terrorism. Curiouser and curiouser!

While we wait for the FOIA process to play out, we thought we'd share what we know with the world. Obviously, the FBI isn't too keen on doing that.

Sparks

Ideas

Dear *2600*:

I very much enjoy reading digests in EPUB format. Are there any plans to keep publishing them for years before 2012?

XCM

If we can streamline the process, we'd be glad to. Part of the problem is that earlier issues were scanned as images and have not been OCRed to as accurate a degree as we would need. It's on our huge list.

Dear *2600*:

I think offering *2600* stickers on your store would be pretty cool! I would definitely buy a few to slap on my laptop and other stuff.

Edgar

We agree. If we can come up with a design we're happy with, expect to see these.

Dear *2600*:

I am a cartoonist from Australia. I was just wondering if you accept cartoons as submissions? I notice it's something that is missing from your magazine.

Glenn

If it was relevant to the hacker community, we would certainly consider such a submission.

Dear *2600*:

Is there any way to search/browse the *2600* archives based on text or topics? I'd love to pick up some back issues with relevant articles, but I haven't run into any way to really dig through the archives to find them.

Cody

Having such a tool would be great for us as well as our readers. For now, the best way to do this is to enter a desired topic into the search bar at store.2600.com, which will yield any issue with that string (in addition to HOPE talks since they also appear on the store). We hope to develop something a bit more snazzy in the future.

Dear *2600*:

What this country needs is a programmable POTS phone for our older family members that can be set up by plugging into our laptops and using simple software. That way people at the house can't change the programming and cause problems. The dial should have four buttons, three of which are labeled 1 through 3, and one big one labeled 911.

The normal keyboard is on the bottom of the phone for you to use when visiting, but is never shown to Mother so that she can never call in to QVC and other places that sell on TV. The great thing about this phone is that the buttons can be set to your number, your sister's number, and the number of her closest friend. Thus, she is protected from herself.

Incoming calls from numbers besides the programmed outgoing numbers don't trigger the ringer, but are given a number to call instead. This removes scam calls.

If she needs to call out for food, you can program that number into button 3. Having only one place to call for takeout can help prevent duplicate food orders (been there!).

Recording all the numbers of calls coming and going would help keep things under control.

If you hackers see or know of something like this that works on a POTS line, let's hear about it.

Dale

Please don't take this the wrong way, but what you're describing sounds a bit like hell. This is why it's so important for hackers to take their skills into old age so that if one of their kids sets them up with something like this, they'll be able to hack their way out of it somehow.

Of course, we don't know what situation you may be in where something this strict might be necessary. We hope that in most cases, a system with more options would be the goal. We'd love to hear some reader ideas.

Dear *2600*:

Abandon Facebook. Embrace Fediverse. When lines are redrawn, look for openings.

Anonymous

Great. Fortune cookies are now sending us postcards.

Meeting Reboots

Dear *2600*:

Just saw your post on /r/2600 - I've never been to a *2600* meeting but have been a lifelong subscriber to the magazine, taking in information since my early teens.

Last time I checked, the most local *2600* meeting was based in New York City. Is there anything relevant out here on Long Island?

Nick

We're not sure what Reddit post you're responding to, but we're glad people are using that site to spread meeting info. While we don't currently have a meeting on Long Island, that could easily change if someone simply organizes one. In this transitional period where meetings are starting up again, it's a great opportunity to start something new. If you decide to go that route, be sure to read the meeting guidelines on our website before proceeding.

Dear *2600*:

I was told there are no online meetings in the Los Angeles *2600* chapter. I know because I found their Twitter account and asked them. This is fine, but I know there are some online meetings. Which online meetings would you recommend for someone who is new? Could you please provide more information?

Josh

If you have a local meeting that hasn't yet resumed in-person gatherings, it's quite possible they have something online for the interim. If not, then it's rather hard to differentiate another area's online gathering from anyplace else. After all, the reason meetings exist is to meet in person, something we're really looking forward to resuming everywhere.

Dear *2600*:

Regarding monthly meetings, at least here in

the U.S., a lot of places (Target, Starbucks, Kroger) are starting to drop their mask requirements for vaccinated customers and things like pinball tournaments are starting to return. Is there a chance we might see meetings officially reinstated in the next couple of months in light of this?

Shawn

This has already begun as you will see in this edition. But we still have to maintain a level of safety and that will differ from place to place. It's the first step back towards normalcy and we may have to reverse course if things don't go well in the surrounding environment. It's hugely important that we all do everything we can to get past this. (It is indeed a good sign to see the pinball tournaments return.)

Dear *2600*:

I'm a coder in Chicago and I'm looking forward to meetings being restored. Please let me know where in Illinois to be and at what time.

Paulie

Well, you're not going to get a call with marching orders. What we suggest is that you keep an eye on www.2600.com/meetings which is being updated frequently, both with locations and with updates based on the health conditions of various parts of the world. Chicago should be listed soon if it isn't already.

Dear *2600*:

It's good to be back in business. We had six people (and two dogs) attend last night's meeting (July) in Raleigh, North Carolina.

arcane

Great to hear! And we do intend to be more welcoming to dogs in the post-pandemic world.

Dear *2600*:

Hi there. We inform you that the domain of our community has changed. It is 2600ptz.ru for now. We also want to assure you that 40 percent plus vaccinated people will attend our meetings at 7:00 pm at Good Place, pr. Pervomayskiy, 2. Otherwise, we will hold them online.

Meetings *2600* Petrozavodsk

At press time, the vaccination rate in Russia was around 15 percent, which is significantly lower than it needs to be in order for a meeting to be officially listed. When that number passes 40 percent, we'll start relisting. When that happens, we hope only people who are completely vaccinated will attend, since it still won't be safe for unvaccinated people. We really look forward to getting back to normal. How soon that happens is up to all of us.

Memories

Dear *2600*:

Perhaps someone here has heard of this early form of computer art. When I was at Purdue in the mid 70s, they used to format the computer printout to form images - not with individual pixels, but with letters. Sometimes in more advanced versions, say if the portrait was of Jesus, the text would spell out "The Lord's Prayer" or some such. They called this art form "Gould." I guess that is how they spelled it. I never saw it written out. Anyway, Google as I might, I can find zero reference to this retro art form. Was the practice of "Gould" limited to Purdue? Does it have another name? Does anyone know any more about this art form?

Robert

In the early days of computing, printing out pictures using ASCII characters was a fun activity and there were all sorts of programs that could do this, even using specific characters like you mentioned. While we're not familiar with that particular program name, a little research shows that a company named Gould provided computers for Purdue, including one called the Gould PN90/80. So it's possible the artwork was named after the machine that it was produced on at that institution.

Dear *2600*:

I am a collector of old school phreaking software for 8/16-bit machines. I know back in the day *2600* used to have sort of a classified section in the back of the mag. Was just curious if that still exists and what the cost for posting an ad is?

info

Back in the day, none of us thought we were actually in the day. Which is why we like to think that maybe we're in it now. Especially since we still do have sort of a classified section in the back and, like always, taking out an ad is totally free for subscribers.

Premonitions

Dear *2600*:

Does anyone remember Slashdot? Remember how it became saturated with pro-Microsoft, British-centric content? Remember how it just faded away? Same thing is happening to *2600* on Facebook.

Tim

If that's true, shouldn't everyone involved be getting some sort of a massive payout at some point?

Dear *2600*:

Someday, automated 18-wheelers will fill the highways. At some point, they won't even have a human supervisor. Is there any reason there won't be highway pirates? What's to stop people from forcing such a truck to stop so they can rob it unopposed?

Lippe

There are definitely some interesting times ahead.

Thoughts on Articles

Dear *2600*:

I just read the interesting Bitcoin article that claimed Bitcoin is completely unregulated. That may have been true when it was written, but it's becoming less true. On March 19, the FBI raided the studios of online radio stream LRN.FM and a convenience store in Keene, New Hampshire. Six were arrested and Bitcoin ATM machines were confiscated. All six were political activists trying to establish Bitcoin as a viable local currency alternative to the U.S. dollar. One of the charges is running an "unlicensed money transmitting business." So apparently the feds now believe you need a license to exchange Bitcoin. Furthermore, the IRS has begun asking on the 1040 form if you received or sold crypto during the tax year. Asking if you sold it makes sense since that generates income. But there are no other investment assets where the IRS asks if you acquired it, nor are any so front and center on the basic 1040 form everyone fills out. While I've seen no moves from the feds to stop what the article discussed of banks manipulating Bitcoin for their own profit, going after a small radio talk show host and a trans anarchist Satanist (two of the people arrested) for making Bitcoin popular in a

small town seems to be the regulator priority.

David

Everything is perception. Someone "trying to establish Bitcoin as a viable local currency alternative to the U.S. dollar" or "operating a multi-million dollar Bitcoin exchange business that facilitated laundering money from scammers across the country [who] even allegedly used the churches [they] started to launder funds as 'donations'"? We don't know either way. Regarding the 1040 question, this comes from the Internal Revenue Service: "If your only transactions involving virtual currency during 2020 were purchases of virtual currency with real currency, you are not required to answer yes to the Form 1040 question."

Dear *2600*:

In response to the 37:4 article by Diana K, yes, I've had the same idea for many years now, but perhaps in more modest terms. I'd like to build a social networking app that incorporates the concepts you describe: anonymity, control over who sees what, etc.

There are technical problems, but I think they are solvable. Anonymity is not as easy as it appears, for one thing. Virtually all Internet traffic is monitored, recorded, archived, sold, etc. by somebody, and it is impossible to do true anonymous routing without reverting to encryption, IP abstraction, and so on. Tor is a step, as well as the blockchain you mention, so it is hopeful that technical solutions could be found that would allow true anonymity without the possibility of someone snooping, mining your data, selling it, and tracking your habits.

But even if you solve the technical issues, there remains one big one: the money. Servers, network bandwidth, hosting, and other essentials don't come free and must be paid for somehow. With a completely anonymous (and supposedly free) service, you lose the ability to raise money from either individuals or investors. The fact that Facebook and Google are some of the wealthiest IT companies in history attests to the ability of using people's data and habits to attract investors, advertisers, and product vendors which fuel the social media monetary "ecosystem."

But back to anonymity: it's a powerful and desirable concept, but the social fabric of being online doesn't lend itself to total anonymity. After all, I don't want to have a social relationship (off or online) with someone who is completely unknown to me. The only way I can see the concept working is that you let selected people into your "circle" or community, and that requires that some anonymity be sacrificed, at least within the limits you set. If you don't, then you might as well be talking to someone with a hood over their face, body, and personality - not a very desirable place to be. However, within your selected community, you would expect that your conversations and exchanges would be private and kept private, and not be mined or monitored by any other entities.

Things do get tricky, though. The reality of such a system requires that you build multiple circles of friends, each with their own privacy or privilege settings. Some "friends" are allowed more access, and some are allowed less. As trust builds or diminishes, you move them closer or further out - or out completely.

Such a system could be built (I've been building software, online and off, for 30 plus years), but the technical and monetary issues are still challenges....

In any case, I liked your article, and it keeps the flickering flame of possibility alive, so keep going.

Chuck

We all appreciate the feedback, encouragement, and inspiration. Thanks for reading.

Dear *2600*:

Thank you for publishing the Reality Winner article (35:3). Sorry I cannot get reliable or better info to create a solid article on aviation computer and network security. I am blocked out.

marc

We don't really know what that means, but thanks for the sentiment.

Dear *2600*:

Your article on the January 6th nonsense said the message would push away some readers, and that was OK. Some will be pushed away because they believe all the QAnon nonsense. Yes, they are worth leaving behind. But another group will be bothered by uneven coverage of political violence.

Which party you support now determines which form of political violence you accept. When I marched against Bush's wars 20 years ago, I always saw violent provocateurs show up to incite violence at our events. We see the same today. For example, the guys from the Revolutionary Communist Party (www.revcom.us) call for overthrowing the U.S. government. I've heard speeches from Chairman Avakian where it's clear he sees inciting race riots as a means of overthrowing our government, i.e., an insurrection like we saw on January 6th. They were one of those violent groups I saw 20 years ago, and today I often see their t-shirts and signs at Black Lives Matter protests that turn into riots. Given the official BLM organization (which we should separate from the broader BLM cause) is co-organized by a self-described Marxist, it's hard to think this is just coincidence. There's video of a Zoom call where activist group Sunrise taught youth that burning down buildings is an acceptable form of expression. A prominent New York congresswoman was on that call and was OK with it. This position is echoed by the magazine *The Nation* (see "In Defense of Destroying Property"). There are lies and non-reality on the left. Their arguments defending their violence don't hold up to factual scrutiny either. Yes, QAnon kooks are much further down the rabbit hole of non-reality, but that does not excuse diminishing the danger of political violence from the other side.

Karl Popper put it well when he asked if a tolerant society can tolerate intolerance. He argued that all expressions must be tolerated until the speaker crosses the line of using coercion: violence, intimidation, etc. A tolerant society must be intolerant of coercive acts. If not, the coercive faction will crush the tolerant ones. If you believe justice can only be served by storming the Capitol building, overturning elections, looting Target, burning down local black-owned businesses, or inciting riots as step one of overthrowing the entire system, then society has a duty to be intolerant of you.

Enrico

There's no question that there are lunatics and destructive types in every camp. But there are a few

things to consider. One is a matter of degree. Ten people spouting nonsense is a whole lot different than thousands. Since you'll almost always be able to find those ten, it becomes rather easy to see a moral equivalency where one doesn't exist. Another consideration is assumption through affiliation. Simply because someone is at an event where a few people are being irresponsible doesn't mean they are in line with that view. Being on a Zoom call is not an endorsement of everything said by others. And being a Marxist isn't an indication in any way that someone is prone to violence.

Such assumptions are naive and harmful, regardless of which side they're coming from. Also, concerning that Zoom call, we understand that it was very deceptively edited by the conspiracy theorists at InfoWars, which pretty much erases any credibility it might have had. For instance, they attempted to make it appear that the participants were planning a coup when in fact they were discussing how to prevent an attempted coup from the other side, a scenario now backed up by the testimony of people on the inside.

It's also deceptive to say a magazine echoed a particular position simply because they printed an opinion piece by someone else. That would be like saying we echo everything in this letter because we printed it.

While some of your points are quite valid, others are buying into well-known manipulation and falsehoods.

Dear *2600*:

One comment to Michaleen Garda's excellent article in 38:1 ("Picture This"): the author argues that hardware manufacturers should include a lens cap by default for webcams. I would suggest that a hardware switch would also be a great countermeasure. Purism does so for PCs and phones: puri.sm/learn/hardware-kill-switches/.

XCM

Dear *2600*:

In 38:1 I saw some pretty angry letters about your "Errors in Freedom" editorial, and have a few comments.

First, I think it's great that the authors of those letters had the courage and passion to write such letters, and articulate their views without resorting to name calling and logical fallacies.

Second, the fact that you both printed the letters and responded to their actual content - rather than what you wished the content were - supports the argument that you do in fact encourage free speech for ideas with which you disagree. After seeing so many instances of "news" sites selectively deleting comments, or companies simply disabling the ability to respond, it was nice to see an actual good faith argument in print.

Third, we need to be able to disagree and, at least within American discourse, the *2600* letters section seems to be one of the last places where that is possible without fear of unreasonable retribution. No two people agree on everything, and if we're not able to engage in speech to disagree, we will inevitably engage in violence.

Finally, one comment on the Big Tech problem. In my opinion, the issue with Big Tech is not necessarily censorship, because we don't have evidence they are censoring anything. In fact, the real issue is that we don't have any evidence of what they are doing at all! Big Tech needs to be more transparent about what they do and why they do it. As far as I know, there is no appeals process, nor is there a way to contact anyone at these companies when a problem happens. If Twitter can't even figure out how to verify @2600, how can we rely on them to do anything else right?

aestetix

We agree that more transparency is needed, but also understand why there's a reluctance to personally address millions of questions and complaints. We believe the solution could lie in empowering users to help solve some of the issues, Twitter being a great example for this. We have more to say on the subject, but we'll wait until we get verified. Any day now.

Dear *2600*:

I noticed in 38:1 that you are displaying code with smart quotes (also known as curly quotes) instead of straight quotes. Smart quotes are the type where the left and right quotation marks are different, slanting inward towards the text they delineate. This is probably not a good idea, because it makes the software syntax invalid. Programming languages and shells know that a curly quote like " (U+201C in Unicode, “ in HTML) is different from a straight quote like " (U+0022), and ditto for an apostrophe or single quotation mark.

For example, on page 11 we find a shell script. In /bin/sh, a construct like "usage: ..." is invalid, and should instead be "usage: ...".

On page 15 you have a C# extract. Similarly, you have invalid syntax: "Authorization" instead of "Authorization".

It's great that you are using a monospace font for code, but please reconsider the use of smart quotes. Python, C, and other languages will yield syntax errors when these types of quotation marks are used instead of straight quotes. Ditto for HTML syntax: curly quotes are OK in the text of documents, but not constructs such as a link.

I respectfully suggest you avoid such typography. Smart quotes are desirable in the text of articles, but not for code.

Speaking of which, I noticed that https://www.2600.com/code doesn't seem to be updated anymore. Is code going someplace else now?

Estragon

You have no idea what a pain in the ass this has been over the years. Even when we get it right, software sometimes "intelligently" makes corrections and we wind up displaying it wrong. We believe the website is displaying code properly, another reason we really need to keep that up to date.

We checked the specific examples you cite and they are in fact wrong in print, albeit really simple to fix when transcribing. However, that's not how they were submitted to the desktop publishing software, which apparently decided on its own to make this change. It would appear this has been ongoing for a long time. An investigation is underway.

Dear *2600*:

In your reply to 6NdLXzc2, you say you are proud of the label of PITA to the bad guys! I'm proud of you too and have been for years.

I think your views are probably the dominant ones in the hacker community, but not among the police and security business folks. Or even the professional who turned skills into money. And forgot their roots!

I always figured that a whole lot of your subscribers were cops and rent-a-cops and such. If they cancel their subscription and can't lurk any more, good riddance!

I've thought before of writing in support, and may have but usually if someone is doing the right thing we take if for granted. That's what you are supposed to do! Keep it up!

OWA

Thanks for the support. But let's not be too quick to make assumptions as to what types of people are holding particular viewpoints. This is where we always get into trouble. The fact is that people will always surprise you with their views, interests, and perceptions, regardless of their jobs or geographical locations. Our supporters (and detractors) come from all corners. What gives us the most hope is the fact that individuals exist everywhere. It's our job to encourage them to speak out without anyone else telling them what to say or believe. If we had more of that, we'd probably have less of the crap we're currently experiencing.

Dear *2600*:

In 34:2, you published a brilliant article by p4b10 entitled "The Censorship Resistant Internet, Part 1: How to Run a Tor Hidden Service (a.k.a. .onion)." In 35:1, you published "The Censorship Resistant Internet, Part 2: How to Run an I2P Hidden Service." The first article stated that this would be a series of four articles on how to run censorship resistant services on the Internet. But four long years have passed and the other two promised articles in the four part series have yet to be published. These two articles are truly outstanding in every way. I learned a great deal from them and they opened my mind into looking at this type of technology and exploring this type of technology in ways that I had never imagined. In ways that I never knew were even possible. So please publish the promised remaining two in this four part series! Solid information like this has never been needed more than *now*! Thanks for publishing the best magazine ever!

The Unignorant_One

This is why it's so important to provide feedback. Hopefully, the author sees this and submits the remaining parts. We look forward to seeing them.

Gratitude

Dear *2600*:

You should thank Justine at Sky's Edge for helping me remember about *2600*. Many years ago, almost BC (Before Computers), I read the hardcopy of your magazine. I recently ordered her rotary cell phone kit and found you on her blog.

Mark

We are indeed grateful for any mention and encourage people to visit skysedge.com.

Dear *2600*:

Thank you for your unending dedication to our community. I've been a subscription (and storefront) purchaser since 1994. With everything we've *all* had to deal with in the past year (especially), I'm just so thankful that you have all managed to publish, or even barely managed to.... We would all be lost without you, and that's not just a statement I'd make from the prospect of losing some source of entertainment. The community would really falter without each and every one of you making sure that *2600* continues. I thank you from the entirety of my heart. Without *2600* I am just some guy with interests no one else understands or cares about. I know I'm not alone when I say how grateful I am that the bedrock of our community has always found a way to move past even the seemingly insurmountable challenges. You have shown us all that there's always a way. I feel like I'm thanking immediate family members here for just continuing to remain in my life. Thank *you!!*

Al

We appreciate those very kind sentiments, but we don't really deserve so much credit. Rather, it's the entire community that we should all be thankful for. We wouldn't have survived this past year without it and we know that there are so many individuals who have been similarly bolstered by the existence of supportive people like yourself. We can never underestimate that power and we only hope it's always used in a positive way.

Dear *2600*:

It's a wonderful day when you receive every back issue of *2600* plus the new one all at the same time!! I think I'm also going to enjoy my lifetime subscription. 1995 me would be proud!

Dan

And don't forget the fact that you're supporting our efforts by getting all those issues. We hope you enjoy every last one.

Dear *2600*:

I have had a lifetime subscription to *2600* for many years. I am starting to feel I should purchase another one. Maybe I will. I am getting so much for my money that I'm starting to feel that I've taken advantage of you.

I read your replies to the various science deniers and accusatory libertarians with particular admiration and gratitude for words well-written.

I am an anti-authoritarian. I dropped out of high school and wrote a book about self-education (it took 26 years to write but was eventually published by a major New York publisher before being read by nobody). My expertise is in software testing, but as part of that I teach critical thinking. I have no credentials or certifications to speak of. I think for myself. I was also the youngest manager in the R&D division at Apple Computer in 1987, so I hope that gives me some shred of cred for what I will say in the next paragraph:

I proceed with confidence in my buccaneering kind of education, and yet I have no trouble believing that experts exist and that I should be guided by them. I am not qualified to directly challenge the things that an expert says when his expertise obviously exceeds my own and there is no compelling evidence of bad faith on his part. Instead I have developed what all responsible thinkers must develop: a constructive kind of skepticism which encourages curiosity and learning, while discouraging strong commitments to any one final account of the truth. I think this is exactly the sort of attitude that Richard Feynman wrote and lectured about. I want to be like Feynman.

I read papers on the epidemiology of the SARS-

CoV-2 virus, not because I was trying to second guess the WHO, but because I was trying to understand what they were saying. I didn't just hear Fauci saying masks weren't important; I found out *why* he said that and what he meant. When he later said they were important, I knew that this represented a change in the public communication strategy in the face of a growing scourge, and not skullduggery. (Early advice was meant to discourage competition for N95 masks, and was focused on protecting yourself; later advice related to cloth masks and protecting others.)

The mistake that many otherwise clever people make is that they think they see a pattern in the data, and then they fall into a self-reinforcing story, surrounding itself with generic immunity from disproof. This is really an emotional failing. It's fear-motivated behavior. It's a need to cling to order for its own sake, in a sea of perceived chaos.

Anthony Fauci is a good scientist. Serious electoral tampering did not occur on the Democratic side (investigations into Trumpian tampering are ongoing on federal and state levels). I don't say these things because I download my opinions from the mainstream media. I say these things because of a compelling *pattern* of evidence from *reputable* sources, combined with the inability of highly motivated actors to muster a similarly compelling fact pattern that points anywhere else. I will change my mind about these things if evidence emerges that can overcome the prior probability of being the result of a QAnon-style smear campaign. (So many people on the right have completely blown their integrity and credibility.)

Facts are social constructions, but that doesn't mean they are arbitrary. It means we must struggle to debug our judgment processes and curate our sources if we wish to live in reality. One of my sources is this magazine (it helps expand what I believe is possible to do with technology). And one of the pleasures of reading is seeing you, Mr. Editor, demonstrate a well-balanced mind.

Thanks!

James

Thank you for making these points better than we ever could.

Dear *2600*:

Greetings from the U.K. As a teenager in the spring of 2000, I came across your magazine on the shelves of a bookstore while on a family vacation in New York City. I was already aware of your existence, but to see an issue of *2600* "in the flesh" was so exotic! Nothing like this would ever be found in the shops back home, as I'm sure you're aware. I was too young to have experienced the BBS days or to have used a blue box, so instead I grew up on dial-up Internet and IRC. I installed Linux on an old 486 PC. I briefly fancied myself as the glorified Hollywood hacker stereotype. I taught myself C++ and joined the corporate rat race. Now I can afford a subscription.

I watched in horror at the rise of the far right in your country, Trump, Charlottesville, shameless police brutality, the feds in Portland, and eventually, January 6th. And so it was that while reading your most recent issue (38:1), I was struck by the intelligence, compassion, wit, and irreverence displayed on every page, but especially in responding to the backlash for "becoming too political," whatever that means. Thank you. A lot has changed in 21 years, but you're still the same *2600*, albeit adapted to the world we now live in. Which is not to say that my country doesn't have problems of its own. But as corny as it sounds, you give me hope for a brighter tomorrow.

oktal

It makes such a difference to know there are people out there who appreciate what we do and who truly get where we're coming from. Thanks for the kind words and for illustrating so well where we've fit in over the years.

Inquiries

Dear *2600*:

Do IT folks have strong intuition as in the ability to determine a problem's cause without the normal troubleshooting procedure? I'd be intrigued if this is indeed the case and wonder if it applies to other trades like mechanics, etc.

Andre

A certain amount of intuition exists in almost any field. When you become familiar with a device or software, it's not unusual to recognize symptoms or behavior and figure out a way to solve the problem before going through a formal process. It basically goes along with taking an interest and developing skills.

Dear *2600*:

Has anyone heard any chatter about these counterfeit bank notes made with plates stolen from the treasury/mint? They have no RFID strip and embossed fingerprints embedded in the print. Over a year in circulation now, at least here in California. I contacted Secret Service, the Treasury, the Mint, and DoJ, and haven't received any replies from any of them - no phone calls, no emails, nothing, not even a weak lie. Nothing on Google about it. I assume it's censored because it's an open case. There are so many of them that real bills can't be found; every bank is participating in the circulation. Just wondering if hackers get access to censored news like this.

Phineas

OK, we'll bite. If this news is censored everywhere, just how exactly did you come across it? As for chatter, we believe you may have just started that. Concerning RFID strips in non-counterfeit money, we don't believe anyone is officially doing that - yet. The technology is there for it, though.

Dear *2600*:

So I have to ask, but why, Hollywood? How badly they show tech in TV shows! I've been watching *Person of Interest.* The one thing that bugs me is how they clone phones. They keep saying things like "I can't clone his phone because he has Bluetooth turned off." Again, I know it's Hollywood, but can someone clone a phone with Bluetooth? Anyway, I had to ask. I know a lot of people install Kali on phones, but to walk close to someone and just clone their phone seems a bit easy. But I know it's for the plot of the show and not the real world.

Chuck

Yes, Bluetooth can be used in this way, but how they present it on television is an oversimplification. Most TV shows and movies shoot for technical accuracy that basically uses some of the right words and outcomes without any other basis in reality. We can understand why, too. Their audience really

doesn't care about that aspect of the story. But every now and then, a gem comes along that takes the time to get it right without slowing down the plot. They are very few and far between.

Dear *2600*:

I have been unable to get the audio MP3 version of your 2020 HOPE conference audio on DVD. If you would please make the conference audio available in full on DVDs, I will commit to buy 30 copies from you. Thank you very much.

MS

For what 30 DVDs would cost, you could just get the entire conference (audio and video) on thumb drives and make a bunch of copies. We didn't make DVDs this time because demand for them is so low and they take a huge amount of time and effort to produce. Like anything else, if the demand is there, we'll consider embarking on this project. If this solution doesn't work for you, let us know why and we'll see if we can come up with more options.

Dear *2600*:

WHY IS CHINA INVESTING HEAVILY IN QUANTUM COMPUTING?

Max

It bugs the hell out of you, doesn't it?

Dear *2600*:

I was going to submit an article but couldn't find any information on the *2600* website about how to submit it. Would you prefer the article be "inlined" in my email, or as an attachment (pdf, doc, odf)? Part of the article has pictures as well - not sure if that impacts the preferred submission type.

braknurr

We really have to improve our website. We've been publishing for nearly 38 years; you would think we'd make it easy to find such information. Basically, any format should work, but it's always wise to send along a pure text version just in case we run into difficulties. Pictures and diagrams are great, but be sure to also include them as separate files in case there's an issue extracting them. We're looking forward to seeing your article!

Dear *2600*:

I have recently become a subscriber to this magazine and I have really been enjoying it! I wish I'd known sooner about it. I am incarcerated and have recently moved to another housing unit where I get better radio reception, meaning I can finally listen to *Off The Hook*! I was wondering, would it be possible for you to add the podcast to the JPay music store? We are able to purchase media from JPay here and listen to it on crippled Android tablets. I would love to listen to past episodes, and there are numerous others here who can't get radio reception due to the noisy fluorescent light ballasts that are in other areas of the building. If this is something you are willing to do, here's some information that may help you get started because JPay is notoriously silent to requests for help.

JPay uses a company called Neurotic Media LLC for their media store. Two services I've heard of, but have not personally verified to be useful in this case, are TuneCore and Urbanlife Distribution. They allegedly are gateways to getting media added to online music stores, because for whatever bureaucratic BS reasons it seems impossible to just go directly to the music distributors and add media yourself. Anyway, hopefully this is not too unreasonable of a request. The *2600* fans here really appreciate your time!

James S.

We can look into this, but we don't feel right having inmates charged for something that's free. Plus we've heard lots of bad things about this company, which has been accused of preying on those least able to protect themselves. We welcome other input on this idea.

Dear *2600*:

Loving my two *2600* shirts (government seal and blue box). Got anything new in the works? Would love to see some new designs or re-releases of old ones.

Daniel

We're definitely overdue for a new design. We're also very open to ideas.

Dear *2600*:

I trust this message finds you well, and hopefully in good health. I am considering a submission to *2600*, specifically an article about nitty-gritty, old-school, get your hands dirty, steganographic encryption involving nothing more than a pen, paper, and a good mind. The problem is I can only type it out or write it with pen and paper in order to show some of the methods used. I know this is a pain in the tuchus to transpose and was wondering if you had any other ideas. Really, I can only use these methods, and email might not translate correctly through this service (I am in prison and utilizing an outside source to forward to you). Any help you may be able to provide would be much appreciated.

Christopher

We accept articles written in all formats, including typewriter, pen and paper, etc., so no worries on that front.

Dear *2600*:

Two friends posted in the last 24 hours that they had been hacked on Facebook. Is there any platform where this is such an everyday occurrence for the average (non-techy) person? Is it just that Facebook is the platform of choice for us old folk? Or the target of choice because there are all these old folks on it?

Shae

The first thing to do is define what is meant by "hacked." Was their password compromised? If so, then how the user is securing it is the first thing to look at. If by "hacked," you mean they were tricked into doing something they shouldn't have done by another Facebook user, then again it's on the user to be more careful and less trusting. If you're referring to having bits of their private life suddenly known by complete strangers, then they should look at how they're sharing that info in their profile. It really should only be between people who are trusted. Of course, that doesn't stop Facebook from messing up the settings and undoing our efforts. And their very existence is perhaps the biggest security hole of all. The sheer amount of people who use it are what make it such a target. But making sure you're following the best security procedures on an individual level will at least confirm that any problems aren't because of anything you've done. It's really not an age issue.

Dear *2600*:

I'm new to programing. I went to the code section of the site and saw all types of code from 2004 to 2017. How can I learn all this? Where do I start so

I can use this code? I just need you to point to my north star. Thanks!

CK

The only way is to read the articles that are attached to the code and experiment. Then read some more and converse with others who are doing the same thing. You never know what might happen.

Observations

Dear *2600*:

I saw that *2600* posted the following on Twitter:

"- We believe in science.
- We support removing fascists from platforms.
- We want monopolies broken up.
- And we demand accountability.
Saying these things really pissed a lot of people off. So we're saying them again in case we missed anyone."

This struck me as completely antithetical to the *2600* that I've been reading since the early 1990s.

1) The statement "We believe in science" is actually the most anti-science statement you could make. Science does not require belief. Indeed, science *rejects* belief as a basis for anything. Stating that you believe in science means that you understand science to require religious faith. Thus, *2600* is, in effect, actually saying here that it is pro-religion and anti-science.

2) The statement "We support removing fascists from platforms" is unarguably pro-censorship and obvious viewpoint discrimination. Now, we can agree that we find such speech reprehensible, but who gets to decide what or who is a fascist? The reason we believe in freedom of expression in this country is because we understand that everyone sees things differently. The marketplace of ideas concept is there so that we can have open discussion on these viewpoints and arrive at a better understanding not only of the truth, but of each other. Ostracization and isolation don't work.

3) The statement "We want monopolies broken up" is pro-big government interference in private affairs. The United States has a terrible track record with antitrust enforcement and there is substantial scholarship that demonstrates that antitrust actions by the U.S. government has actually had the effect of stifling competition, rather than promoting it. *2600* has historically wanted the government to stay out of people's business.

4) The statement "we demand accountability" seems to be pro-law enforcement overreach. Who is administering this accountability? And what is it accountability for? This needs more explanation.

In the end, I never would have expected to see *2600*, in one tweet, signal a change to becoming pro-religion, pro-censorship, pro-big government, and pro-law enforcement. I'm just shocked by this.

I'm willing to believe this might be the result of some inarticulate writing, but *2600* should put something out to clear this up.

olightg32

Wow. Seriously, thanks for the laugh. We definitely needed it.

In case any of this was serious, let's go over some things.

1) So saying we believe in science means we are anti-science. Makes about as much sense as anything our detractors have been saying lately. (We meant the opposite of that - are we doing this right?)

2) Imprisoning a fascist for expressing their opinion would be censorship. Kicking them off Twitter or Facebook is entirely within the rights of those platforms. And other users are entirely within their rights to pressure those platforms to act. As for who gets to decide what defines a fascist, we'll simply ask you where the line is. It has to be somewhere, right? The "marketplace of ideas" concept is great until it gets overrun by hatred, ignorance, and fear. Then it becomes a Fox message board that's incapable of addressing any issue without devolving into racism or nationalism. Let's try something else.

3) Who says you have to be pro-big government to be anti-monopoly? Well, you do, apparently, but we don't buy into that. You need governments to break up monopolies. And you need people to change governments. And you need monopolies for nothing at all. It's just too bad we can't fit that on a bumper sticker.

4) This feels like your first point all over again. So saying you want accountability means you are pro-law enforcement? What if it's law enforcement you want accountability from? The twisted logic here is dizzying.

Overall though, this has been a fun jaunt through bizarre conclusions and misassumptions. Time to get serious again.

Dear *2600*:

I was at the cardiologist today and they went ahead and did a 12-lead EKG as part of the nurse visit so it would be ready for the doc to do the doc thing. Well, the nurse kept replacing the arm and leg leads in different places and wasn't saying anything about what was going on, so I asked. She said she was getting a lot of interference. I thought for a second as to what had changed since the last time I was there. The only thing I could think of was that I got an iPhone 12 the previous week. It had been a long time coming (was still rocking the 6s!) but when my old phone started going nutzo, it had to happen.

So, as a test, I put my phone behind my head under the pillow to get it away from my torso since every one of those electrodes basically made up a circle of where they were trying to pick up minute electrical signals while there was my phone leaning on the fence around my torso with a music-festival-sized rig just pumping in this radio signal that would appear as static to their EKG machine. Sure enough, it was clear.

The nurse said in 15 years of being a cardiac nurse, she'd never seen a phone interfere with a totally wired EKG (from patient to machine). She wrote that discovery down on a post-it note and was going to bring up iPhone 12s at the next staff meeting. She also said that mine was the first 12 that she knew of where a patient had one in their pocket. I'm kinda curious now why a 12 would interfere when no other phones have. Any ideas?

Mike

The new MagSafe magnet that comes with the iPhone 12 is apparently the issue. This wireless charging feature has a magnet that can interfere with things like pacemakers. Apple suggests you keep these devices at least six inches away from any implants. That's not nearly far enough for us.

Dear *2600*:

Hi, something strange happened. I experienced a "blip" and something nearby malfunctioned scanning an odd code then went back to normal. It was like for a split second I was in two places at once, but dimly remember a room with spotlights and a high pitched whine. Has anyone else had this happen to them? It's not the first time this has happened. A few years back, I was experimenting with something and that morning walked past three computers that all crashed as I approached them. Fortunately, it doesn't happen that often.

Andre

Either you're actually inside a network television program or you're in a great position to write a script for one.

Dear *2600*:

Ohhh! His name is "Lord Nikon" because he has a photographic memory. I just got that.

Jonny

Twenty-five years later and that film is still giving back.

Dear *2600*:

I used to buy *2600 Magazine* 22-something years ago at the weirdest vendors around the world. That was enough to put you on a watch list back then. Now it's 2021, and after meeting so many brilliant IT professionals, I've realized that I'm not as smart as I like to think I am. Never have been, never will be. I was a late 90s PBX telecom hacker (loosely using the term hacker) into hybrid NEC key systems. I remember getting so excited about the first 802.11 protocol. I burned out so fast. Now I sell planes and real estate. I like that too.

Alex

Don't sell yourself short. Nobody is as smart as others believe them to be. And everyone knows this is true of themselves. In the hacker community, the spirit and inquisitiveness really matter. We think you've still got that or you wouldn't be writing.

Dear *2600*:

Just had a request from our service provider to reconfigure our system in order to publicly publish patch level information so that a company called BitSight will score the provider's "security" better. (Because they can't determine our web server patch levels, they make the assumption that the system is patch deficient, the company is security lame, and provide that assessment to their paying customers.) Apparently, there's now an industry niche with a number of companies that are selling these scores to decision makers regarding companies (who lose business due to low scores) in their sectors. I think their method bakes in bias which ladens their product with errors. On further thought, it kinda seems ready made for a straight up shakedown. Anyone had any experience with BitSight or its peers?

John Smith

This is a great place to start a conversation about them. Maybe your service provider should be a part of it.

Dear *2600*:

I set up an eye appointment for myself this morning and got a text message from the clinic a few hours later asking for my prescriptions, medical conditions, and vision history (with specific instructions to reply to the text message with that info). It's almost like they've never heard of HIPAA.

Dave

There is a ton of good information in the Health Insurance Portability and Accountability Act. Your eye clinic would benefit from a visit to hhs.gov and a few pointers on how to communicate health care info securely.

Dear *2600*:

Everything is messed!!! Please guide. I have messed everything.

fred

Don't worry, we've all had days like that.

Dear *2600*:

Wanna know how badly business owners/executives treat security? I'm a developer and I just did a huge software update for all of my clients. It was focused on security. Yesterday, one of my clients called me and said, "What do I have to do to keep using the older version of your software? I hate all these security features and passwords. If I had my way, no one in the building would need a password to log in." I stopped by his building for a visit. Everyone uses the *same* username and password to log in, and everyone has a post-it on their monitor with the password. This is *not* software running on his local network. This is a hosted app on a remote server. You can log in from any browser!

Robert

Wouldn't they just need a single large post-it note if it was just one username and password? Seriously, this could well be the worst security ever. Watching what happens next could be fun and instructional.

There are times, though, when older versions of software work better or have less annoying features. We've never been fans of pressuring people to move onto something they're either not ready for or don't want at all. In addition to occasionally being mocked, the end user needs to also be listened to.

Dear *2600*:

It's bad enough that a group that has long been an example of "question everything" has become so anti-question. And I find it fascinating that when someone calls you out on this change that you have accused them of "hate." At one point in your response to letters, you accused someone of "pure evil," not for saying actual evil things, but for saying things you don't agree with. Tell them they are a "fan of Trump" because they ask questions and give their own perception, even though they specifically say they aren't a fan. I guess you know better than they do. Another letter also questioned your points, and again you accuse them of "hate." That was twice, with absolutely *zero* evidence whatsoever. Simply because they dared to question the accepted storyline.

Are they wrong? Maybe. Are they right? Maybe. Neither concerns me. What does concern me is a group that once represented "question everything" and "don't believe everything you hear" is now solidly "question nothing or be accused of being evil." One guy literally said "trust the *evidence*." What's so hateful and wrong about that? Is the evidence not enough, we have to just trust the "experts?" I guess we should have trusted the FBI when they told us that hackers were criminals. I

mean, they *are* the experts on criminals.

We have countless examples through our own history of politics defining "truth," only to find that "truth" to later be lies. The Pentagon Papers, Watergate, Bill Clinton "I did not have sex with that woman," Joseph McCarthy... our history is full of reasons why we should *never* take any public official's word at face value.

I find it a real shame to see today how acceptable it is to browbeat and put down others instead of listen. I really hate to see it perpetrated by those that should remember how much it sucked to be treated that way. You used to be about the truth and shining a light on everything so that we can see for ourselves. Know all the information and make our own informed decisions. You're honestly no better than those that tried to contain you. They thought they were doing the right thing and had good reasons, too. They were told by the experts what evil you were and how dangerous you were to us all. I guess we should have kept listening, huh?

Lock

Yes, the diabolical plan is finally coming to fruition. You never should have trusted us. (We know it's risky to use sarcasm in such discussions, but we're not going to change who we are.)

Now then, when ripping us a new one, it's always nice to quote specifics as you hurl accusations. Otherwise we have to try and find out just what it is you're referring to.

Let's start with the "pure evil" remark. We combed through over two years of letters and the only instance we found was from 38:1 where we said: "Blaming groups like Black Lives Matter for everything you dislike only shows how easily you can be convinced that people who are different from you are nothing short of pure evil." This in your world is us calling the letter writer pure evil? It's hard to counter an accusation when what you're accusing us of doesn't exist. Similarly, us saying "For someone who claims not to be a fan of Trump, you've repeated his talking points precisely" is not us calling them a "fan of Trump" but simply questioning their claim not to be based on what they said. And we can find no instances of our accusing someone of hate.

If you want to label us in a particular manner, false accusations that are easily disproved aren't the way to do it, just like false facts that are easily disproved are no way to win an argument on current affairs.

Try harder.

Dear *2600*:

The last issue of *2600 Magazine* epitomizes a "left-wing rag." I won't be renewing my subscription.

Ke

While we don't embrace one wing over another, we're curious if we've ever appeared as anything other than what we appear to be now.

Dear *2600*:

I've been a reader of *The Hacker Quarterly* for several years; every issue has had several outstanding articles that I've really enjoyed, and the letters section has never failed to make me laugh.

Unfortunately, the latest edition I purchased will be my last. A few years ago, there was only one thing you needed to fit in with the *2600* hacker community: the hacker mindset. Recently I've felt a shift, and there are now two things required to fit in with the *2600* hacker community: the hacker mindset and an active hatred of conservatives.

I've never supported Trump, I'm a fan of science-based research, and my political compass is more centrist than it is conservative, but I now feel unwelcome in the *2600* community because I'm not liberal enough - because I don't openly mock conservatives.

The thing that sealed my decision was something in 37:4- it's the "Artificial Interruption" column by Alexander Urbelis. He did a search for domains that contained the words "Trump" and "suck," and one of his... noteworthy... findings was a domain called isucktrumpsdick.com, which redirected to Ted Cruz's Twitter page.

Maybe I'm wrong, and maybe things aren't as bad as I feel like they are, but it's gotten to the point where I personally no longer feel welcome, so I'm out. A year or two ago I would have considered *2600* swag absolutely awesome, but if you decide to print this email in your magazine, don't bother sending me a t-shirt or anything; I'm not sure I want swag from a community that rejects me.

Even so, the people who put together the magazine seem pretty awesome! The opening letter of 37:4 actually made me reconsider some things. For example, I've always considered open forums to be a battlefield of ideas where only the strongest arguments survive, but you likened the current political landscape to a message board full of trolls - disingenuous people who are more interested in causing trouble than in seeking truth, and just as trolls in a message board need to be banned, political trolls need to be silenced.

I'd never thought of it that way, and you're not wrong, but it's also dangerous because so many of us confuse honest people from the opposing political party with disingenuous political trolls (I've seen this happen on both sides of the aisle). And it seems to me that, in the *2600* community, for every person willing to write an insightful article (like yours), there are ten people willing to write articles about how the domain "isucktrumpsdick" redirects to Ted Cruz's Twitter page.

I wish you and *The Hacker Quarterly* the best; maybe I'll be back someday if things change.

Cody

For the record, we don't hate conservatives and we don't believe anyone on our staff does either (including the columnist in question). Hatred is too strong a word to use even for those who we strongly disagree with. What we do hate is what's happened to our society and how people have gone down some pretty dark roads lately, no longer listening to facts, science, or even common decency. From what you've written, you're pretty far from any of that. In fact, you likely have more in common with the people you believe are rejecting you than you do with those who are being mocked. The latter are earning a reputation of fearmongering, ignoring scientific facts, and being willing to overturn democratic elections and keep people from legally voting when it suits them. We understand why it may feel as if you're being included in this, and there are certainly idiots on the non-conservative side who would paint things with an overly broad brush. But conservatives who oppose the anti-science,

anti-fact, pro-Trump-at-all-costs agenda are the real potential heroes here. We support anyone who shows courage by speaking out in what is truly a difficult time for them.

As for the domain cited in the column, this was simply something that was found during the author's research. The fact of where it was directed was humorous to some, obviously not to others. But it's something that would be discovered if you did the same research.

We know things seemed simpler in years past, but it's really the world that has changed more than the hacker community. Had this sort of thing been happening 20 years ago, we're certain most of us would be condemning it in the same way. At least we hope so.

Dear *2600*:

Please update your PGP key. It currently only lists "articles@2600.com" in the UID section and is only 2048-bit.

You should either have separate keys for payphones@2600.com, articles@2600.com, and letters@2600.com *or* have all three email addresses listed in the UID of the new key.

Oh, and the new key should be at least 4096-bit RSA or ECC-based.

Thanks for rockin'!

8261 80CC 3E97

We appreciate the advice, but we're going to keep it as is for a couple of reasons. We want to see how durable PGP actually is. If all it takes is a few years to be able to compromise it, we want to see evidence. From what we've heard, there's still a bit of time before that happens.

Our PGP key is set up for article submissions, not payphones or letters. The latter two don't tend to involve sensitive material. However, someone can use that PGP key when sending to other addresses if they really want to and we'll get it decrypted using the articles key. Not a huge deal for us.

We don't really encourage the use of PGP as a rule because of the high amount of user errors encountered, where either an old, outdated, and impossible to delete key is used instead of the correct one; someone encrypts their file incorrectly and requires a whole lot of back and forth that we just don't have time for; or there's some sort of version incompatibility that needlessly complicates things. For truly sensitive material, we recommend people use our SecureDrop submission process, which is far easier to use and more secure. It's reachable at 2600.securedrop.tor.onion on the Tor browser.

Dear *2600*:

The last few issues of *2600* have seen many a reader's letter complaining about the magazine's political leanings and, while I think it is laughable to expect *2600* to believe President Trump's election lies, I believe there is a valid concern.

The pages of *2600* are full of (healthy) skepticism and hatred for corporations, but significantly more rare is criticism of government. Instead of the age-old hacker ethos of being wary of power structures in general, the new ethos seems to be wary of power structures, but only if they do not conform to our personal morality.

One example is January 6th, where a bunch of sore losers entered a fascist government building without a permission slip, yet the *2600* editors apparently felt personally offended by this, feeling it was an attack on democracy. Why should we care? This was never argued in the pages of *2600*, besides an automatic appeal to democracy - as if democracy isn't often used as a tool of oppression.

Another notable example is the government's COVID response. Millions of people have died from COVID within and outside the United States. There was also a coordinated attempt by powerful people to suppress scientific debate (and misinformation) on the topic. *2600* itself has been guilty of dismissing claims contrary to mainstream consensus without evidence, save for a reference to "science." The editors apparently expect us to listen to the official Oracles at D.C. and blindly trust that their proclamations of Science - that notoriously fickle mistress - are true, even after they have changed policy countless times. Where are the celebrations of people breaking scientific censorship? Surely that is the largest story *2600* could currently run. You apparently had the print space last issue to scold a reader for not following the guidelines surrounding social distancing that came from millionaire bureaucrats (the CDC claimed COVID was not airborne then), yet you cannot devote space to approach the issue with nuance? The tone of *2600* has taken an authoritarian turn as of late, and it emanates from the pages proudly. Do not expect all your readers to go into that good night gently.

CSCII

One thing we can admit to is that we were wrong and naive in our beliefs, conclusions, and expectations. We thought logic and science were enough. We assumed evidence would be convincing. But, in fact, none of that matters when the answer has already been decided.

Two plus two can indeed equal five when it's convenient. That's what we didn't know going into this. We thought we were witnessing a fascist attempt to overturn a legitimate election on January 6th, but apparently it was the building itself that was fascist and the heroes of democracy were those who stormed it. Or, as we're now seeing expressed here, democracy may actually be the problem. Those who embrace science are really the ones working against science, coordinating with other so-called scientists around the globe, and using fake evidence to suppress those who disagree. Never before has it been spelled out so clearly.

What we find particularly amusing in such proclamations is the accusation that we don't criticize government. Apparently the last four years somehow didn't count. Even if we accept that, there isn't an administration since Reagan that we haven't criticized at some point and there has never been one that we've trusted.

Facts are open to interpretation. But they're not open to being rewritten.

Congratulations

Dear *2600*:

It is our pleasure to inform you that HopeNet has been selected as the winner for the 2021 San Francisco awards in the category of Pharmacies. Notification to other award winners in San Francisco will be made over the next several weeks. After all award recipients have been notified, we will post the

complete list of winners on our website.

It is not a requirement, but is your option, to have us send you one of the 2021 awards that have been designed for display at your place of business. As an award recipient, there is no membership requirement. We simply ask each award recipient to pay for the cost of their awards. The revenue generated by the San Francisco Award Program helps to pay for operational support, marketing, and partnership programs for local businesses. There are various award types, sizes, and shipping options.

Bob Kim
San Francisco Award Program

We've seen scams before, but this one takes the cake. Our conference website (hope.net) isn't in San Francisco and sure as hell isn't a pharmacy. And if that's not enough, telling people they've won some kind of award based on absolutely nothing and then turning around and trying to charge them for the privilege is about as low as you can go. Searching online reveals not only that many have fallen for this, but that this isn't limited to San Francisco. This sort of thing is happening everywhere. The Better Business Bureau says "Most legitimate awards do not come with costs to the recipient." And, if this were legit, they would probably have been able to get a better domain than 2021-localbestnotice.org.

Further Info

Dear *2600*:

There was a recent letter asking for information on radio in 37:4. Rather than lay out an article, encouraging exploration may be more useful.

In the U.S., there are a few different types of radio options for civilians. Ham (amateur) radio is just one of them. Other popular options are GMRS/FRS, MURS, and CB.

At a high level, you commonly have VHF, UHF, and HF radio. VHF and UHF are typically local communications (what constitutes local is dependent on transmitter power, antenna types, and various atmospheric conditions). HF is sometimes longer range or global (again, depending on the various conditions).

Amateur radio has spectrum available in VHF/UHF and HF. You can do voice ("phone") communications or send data (look up "digital modes"). Most ham data is relegated to HF, though some modes like APRS are popular on VHF/UHF. You cannot encrypt any data on ham bands. There are three ham licenses and each one gives you permission to operate on more frequencies. Each license level lasts for 15 years and requires a test. Sometimes the tests have a small fee. Most ham radio is typically just old men talking to each other, but sometimes you'll run into the stray hacker. Cherish those moments. I've found a few while working FM satellites with only a handheld radio and an antenna made out of a chopped up tape measure. *The ARRL Operating Manual for Radio Amateurs* provides a good overview of a lot of the possibilities of ham radio.

GMRS is a superset of the FRS frequencies and these are laid out in channels (fixed frequencies). GMRS requires an inexpensive license with no test, and the license covers you and your immediate family for ten years. FRS is license-free. You can run repeaters and use removable antennas with GMRS (but not with FRS). These are both in the VHF/UHF range. These seem to usually be occupied by children with blister pack radios from big box stores, families in caravans, and preppers doing survival comms. No data or encryption is allowed here.

MURS is license-free as of the early 2000s. They're channels on the VHF frequencies. Some data is allowed here, but encryption is not (notice a trend?). Occasionally, large fast food restaurants will use these frequencies for their drive-through ordering.

CB is HF and can sometimes be used nationally, but the legal power restrictions and current solar cycle means you won't be talking around the world. It tends to be filled with a lot of offensive chatting. Almost like a voice-based IRC of the mid to late 90s.

Typically, all of these individual bands have expensive radios that are needed to meet FCC requirements. One can also acquire inexpensive (around $30 USD) VHF/UHF radios with all manner of badging like BaoFeng, Retevis, etc. that can be programmed using a homebrew (or eBay purchased) cable and a piece of free software called CHIRP. Receiving with one of these radios is completely legal without a license for anybody. Transmitting requires proper licensing and in some cases can't be legally done (such as with FRS where there are transmitter output and fixed antenna restrictions).

HF transceivers are usually costly (starting out around $400 USD) but they normally cover ham bands. If you want to use CB, you'll have to have a CB specific radio. If you don't wish to transmit, pick up a "shortwave" radio with SSB capabilities and you should be able to listen to most of the HF spectrum with a long piece of wire for an antenna. These can often be had for as little as $20 USD in some cases, but you get what you pay for.

Software defined radio is also popular and you can do some free listening at websdr.org, though these stations typically only cover ham bands. A scanner, RTL-SDR dongle, or previously mentioned cheap BaoFeng et al radio plus a proper antenna (often assembled from junk parts) would be required for listening to VHF/UHF.

I hope that helps someone out. Each paragraph could probably be its own article. Maybe that'll encourage some folks to write more radio-related content.

TENFOURGOODBUDDY

We hope to encourage you to do just that. You would get a subscription and a shirt for each article you wrote and it seems like you have enough knowledge to write plenty. The radio world has so much of interest and, while things have changed over the years, there is still a great deal that can be done with a little creativity and knowledge. Thanks for this inspiring piece.

WE WANT YOUR LETTERS!

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

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

EFFecting Digital Freedom

by Jason Kelley

You Are Not Being Tracked

On the surface, EFF's website looks pretty much like other sites out there. But underneath the hood, there's a major difference: we aren't tracking you.

The same is true of emails we send out. EFF doesn't include pixel tracking or other embedded trackers to record who opens which emails. And while much of the tech world is busy thinking up new ways to collect your data, we don't intend to change any of these privacy practices. In fact, we think the time is right for every other privacy-focused individual and organization to join us - and that means you, too.

Instead of granular tracking, EFF collects aggregate, anonymized data of our web traffic. This involves very limited logging, but still lets us know, for example, if a lot of traffic is coming from a particular country, or a particular website. We occasionally use session cookies, as well, where it makes sense to do so (for example, when the user is logged in). And we will use logs with full IPs when responding to an attack or technical problem, but unless absolutely necessary even those logs are aggregated and anonymized after seven days. And, with consent, we do get and retain voluntarily provided information about specific users, like our supporters' addresses (when they want to give them - anonymous donations are fine too!). You can read all of what we do in our clear Privacy Policy at `https://www.eff.org/policy`.

"Doesn't this make your work harder?" you may be asking. At times, yes, this lack of info on our users makes our work *very slightly more difficult*. We rely on donors like you to support our work, and as an advocacy organization, we rely on digital activism to get the word out. Having easy access to detailed analytics data about the visitors to our website or the readers of our emails could help us do both of these things. But that would require us to collect large amounts of data about our users, supporters, and followers, and we don't believe the tradeoff is worth it.

Despite this limited data, EFF is an active, growing, and successful organization that's been around for 31 years. And we aren't alone: plenty of other organizations, like the Internet Archive and companies like Basecamp, walk the talk by collecting much more limited data than is common. And we'd like to pose a challenge to others who care about user privacy: turn off overbroad tracking.

For 31 years, EFF has fought to protect the rights of the user - the person who's making use of a technology such as a website, a computer, or a smartphone. Tracking those users, by and large, benefits the company, person, or organization doing the tracking, if at all, not the user on the other end of the technology. Fighting for the user means giving them the control to not be tracked, to remain anonymous or private, and to not have their data collected without their permission. This is even more essential when the technologies are common and extraordinarily popular, like email and the web.

Many companies suggest that pervasive tracking is beneficial for users, because it allows them to be targeted for things that they care about. But this argument robs users of their consent. It assumes that people want to be tracked by default. EFF assumes people do *not* want to be tracked by default. This argument also sidesteps the fact that despite the vast amount of personal information companies collect, they still use this data to derive conclusions that are inaccurate or wrong.

The same is true for the argument that pervasive tracking, for instance, of your email interactions allows an organization to send you better, more effective, perhaps even more personalized emails in the future. This may be true at some level; but this digital tea reading, even when it "works," represents an invasion of privacy that privacy advocates should not take part in. And in a worst case scenario, it could expose your readers' private information to unexpected third parties.

The slow, steady, relentless accumulation of thousands of data points about how we live our lives is a serious threat to our privacy. It can reveal political affiliation, religious belief, sexual identity and activity, race and ethnicity, education level, income bracket, purchasing habits, and physical and mental health. And unfortunately, due to the way that tracking and ad tech works, much of the data collected is often rolled up into a much more detailed profile about a user - even when it's collected by a single website or organization.

But it doesn't have to be that way. If you are building any sort of technology, consider whether or not your users would appreciate being tracked. The answer, we believe, is almost always no. And if the answer is yes, ask for user consent for any tracking you might do. Again, we believe that your users will appreciate this - and that this is their right.

Of course, the problem isn't just yours to solve. Companies that provide analytics tools, content management services, and mailing list management don't offer nearly enough privacy-protecting options, and we believe that's a big part of the issue. It's an insidious ecosystem that needs to be reformed, and along with other advocacy organizations, legislators, and activists like you, we can do it.

On an individual level, the easiest way to get started protecting your users' privacy is to think about what data you actually use. If you would be satisfied with anonymous, aggregate data about your website visitors (we are), or getting general insights about email usage rather than granular data about each recipient, there are options out there. We'll be working on recommendations in the coming months to make it easier for you to switch to more privacy-protecting options. For now, we hope you'll join us in turning off any granular tracking, and letting everyone using your services or technology know: you are not being tracked. Be clear about the data you collect - and why. You'll win points with your users, and you'll help us all move the needle one step closer to a better, privacy-conscious online future.

When 5G Technology and Disinformation Collide

by Kenneth Luck, Ph.D.

If you Google "5G Conspiracy Theories," an endless stream of news stories, blog posts, and videos will populate from your search inquiry, most published throughout 2020, just as the COVID-19 pandemic began to pick up steam around the world.

But the 5G conspiracy theory really got people to pay attention in December 2020, when a lone Tennessean named Anthony Quinn Warner detonated a bomb in front of an AT&T building in downtown Nashville, killing himself and damaging 14 other buildings in the area (Jibilian 2020). Luckily, no one else was killed, but Warner's deranged act was motivated, in part, by his belief that 5G technology (the fifth-generation mobile technology) is harmful.

Werner was a 5G conspiracy theorist.

Like many conspiracy theories, the 5G conspiracy theory has many variants, but the main gist of this conspiracy theory claims that the next generation of mobile technology will be used to spy on Americans, that 5G radio frequencies cause illness in humans and animals, and that 5G technology is the real cause of COVID-19.

The 5G conspiracy theory is nothing more than repackaged junk thinking that can be traced even before wireless network technology has existed. The burden of proof lies with those who make the claim, and, as Carl Sagan once said, the larger the claim, the larger the evidence is needed for one to accept that claim. In this case, 5G conspiracy theorists have turned up empty-handed.

Although exploring the full extent of conspiracy thinking remains outside the scope of this article, it may be helpful to summarize a few key points. First, conspiracy theories often involve a "powerful other" - a person or group who is in *total* control and can exert his or her will easily over others (Luck 2020). Next, conspiracy theorists often feel as if they have some type of "special knowledge," which may make them feel unique (Luck 2020). This "Need for Uniqueness," as the psychology literature calls it, remains attractive to conspiracy theorists. Finally, conspiracy theories often emerge in the wake of major political, social, or historic events (Luck 2020).

The 5G conspiracy theory includes all of the above characteristics, with special emphasis on the last point. Generally speaking, new technology often leaves onlookers astonished, particularly if they don't understand the underlying principles or mechanics of how that technology works.

Once it's here, 5G technology will undoubtedly touch the lives of many individuals. For example, 5G will enable enormous bandwidth, will introduce unprecedented speed, and will spawn many new 5G consumer devices (Russell, et al., 2020). While all of this will generally be a boost, 5G conspiracy theorists have seized on the fact that controversial Chinese telecompanies have been involved in the development of 5G, more towers will need to be installed, and 5G will use a new region of the radio spectrum (Russell, et al., 2020). While the practices of Chinese telecompanies may merit legitimate security questions, the latter two - more towers and a new region of the radio spectrum - remains almost a moot point, as it is in part these two technologies that will enable greater bandwidth and faster connection speeds. Again, there is no credible evidence to support the claims of 5G conspiracies.

It's easy to forget that conspiracy theories cropped up about 5G's predecessors 3G and 4G (Mays 2020). Back in the early 2000s, for instance, some conspiracy theorists tied the 2003 SARS outbreak to 3G wireless technology - and the same false connections are happening now with COVID-19. Researchers refer to this cognitive bias as "the conjunction fallacy" - or, when two co-occurring events take place (like the installation of 5G towers and the coronavirus pandemic), one is thought to be the cause of the other. But this type of reasoning is false, particularly if the claims lack supporting data.

Moreover, whereas the United States has become a hotbed of misinformation and conspiracy theories in recent years, it is worth noting that unlike the QAnon conspiracy, which focuses mostly on U.S. politics, the 5G conspiracy theory is truly a global phenomenon: Early in 2020, reports of individuals physically attacking 5G towers were reported in the U.K. (Goodman and Carmichael, 2020). Meanwhile, around the same time in Bolivia, two telecommunication masts were set ablaze. And in Australia, protesters in May 2020 showed up at anti-COVID-19 lockdown demonstrations with anti-5G signs and placards (Meese, Frith, and Wilken 2020). Additionally, it was reported last year that "conspiracy theories about 5G technology were considered the greatest domestic threat to critical infrastructure [in the U.S.]," (Stunson 2020).

It may turn out that 5G may bring some advantages and some unforeseen disadvantages, but this remains the case for almost any new technology. In fact, the technology adoption curve is almost the same for any new innovation. As the sociologist E.M. Rogers pointed out in 1962, there are the innovators, early adopters, and laggers, but - ultimately - new technologies eventually end up in all of our hands, even if for some individuals that technology becomes not-so-new by then. Finally, it may also be in the interest of IT professionals, programmers, and anyone else involved in the tech

community to start educating the public about what 5G technology is and how it works because one of the best defenses against misinformation is factual information.

References

- Goodman, J., and Carmichael, F. (2020). "Coronavirus: 5G and microchip conspiracies around the world." *BBC Reality Check*. Retrieved from www.bbc.com/➥news/53191523
- Jibilian, I. (2020). "The accused Nashville suicide bomber was reportedly paranoid about 5G technology. Here's what we know about the false 5G conspiracy that went viral this year." *Business Insider*. Retrieved from www.businessinsider.com/➥anthony-quinn-warner-false-➥5g-conspiracy-theory-nashville-➥bombing-explained-2020-12
- Luck, K. (2020). "Emergence of conspiratorial ideas and big data: A Google NGram Viewer quantitative analysis of historical trends from 1900 to 2008." (Doctoral Dissertation, Marywood University, 2019). *Journal of Applied Professional Studies*.
- Mays, M. (2020). "Why 5G conspiracies are so prevalent." *WKRN*. Retrieved from www.➥wkrn.com/news/local-news/why-➥5g-conspiracy-theories-are-➥so-prevalent/
- Meese, J., Frith, J., and Wilken, R. (2020). "COVID-19, 5G conspiracies and infrastructural futures." *Media International Australia*, 1329878X20952165. Retrieved from doi.➥org/10.1177/1329878X20952165
- Russell, J., Wells, R., Dalby, A., and White, J. (2020). "5G: The Complete Manual." *Marketforce*. London, U.K.
- Stunson, M. (2020). "What is 5G paranoia? Nashville bombing renews conspiracy theories." *Miami Herald*. Retrieved from www.miamiherald.com/news/➥nation-world/national/➥article248131405.html

HOW TO HACK THE AMERICAN MAILZ

by The Last Postman

Most people reading this have used the postal mail service at least a couple of times throughout their lives, or are somewhat familiar with it. But how many have tried hacking the mailz? Of course, all of us know that not everything on the Internet is true and, in 2013, I heard on the interwebz that one could send mail for pennies, so I wanted to see if it was even true and learn how to do it. It was then that I began my journey to become The Last Postman.

I learned that it was indeed true, as I disassembled the many pieces of the mailz, and I wanted to share my findings with my fellow hacker community. I developed this hack, or exploit, in 2013-2014. Remember that people were sending mail in 1863 using this same postage rate, that it's still totally legal and lawful, but that it has been hidden from everyone. So now it's time to free that information! I've sent mail like this from the east coast all the way to Hawaii and I've received one piece of mail back using the same method.

Let's call this the 1863 postal rate, as this is the year it all began. Looking at legislation from the 37th Congress (1863), specifically Session III, Chapter 71[1], we see that Section 22 tells us that we can send mail for three cents per each half ounce. Interesting note that in 1863 you would pay your mail carrier upon mail delivery the three cents, but today we can buy one, two, and three cent stamps, as well as other amounts. I love asking the postal clerk for 100 stamps and then letting them know I need 100 three cent stamps! Remember to weigh your envelope and affix three cents per each half ounce (round up) as per the 1863 "law." Also remember that the government created this rate to regulate an honest business owner named Lysander Spooner out of his mail business, as he was doing a much better job at it and government tends to like to "kill the competition." I encourage you to learn more about him on your own as he is fascinating.

Next, let's explore how to address our mail to do this. I call this a "simplified address," as it does not utilize any abbreviations, as such are believed to be copywritten by the United States Postal Service ("USPS") company. Here is an example:

John-Jacob of the Family Smith
c/o 2600 Sixth Pine Road
Apartment #7A
Boston, Massachusetts
ZIP Code Exempt as per United States Postal Service
Domestic Mail Manual Section 602 1.3 e(2)

Above we see the mention of the USPS's "company manual," called the Domestic Mail Manual ("DMM"), which is the document that lays out their company's policies and prices. The USPS likes to move sections of their manual to hide certain information, as the Section 602 I cite above was previously Section 122. As of Christmas 2020 though, the USPS deleted[2] the specific subsection I cite above, but that does not make it any less valid. It can still be used and this is only clear evidence that they are actively hiding this information from the people. Search on archive.org for the May 2020 snapshot (or earlier) to see it before "deletion."

Since it was "deleted," but still completely valid, I will quote DMM 602 1.3 e(2) here: *"Unless required above, ZIP Codes may be omitted from single-piece price First-Class Mail (including Priority Mail), single-piece price Standard Post, and pieces bearing a simplified address."* We're using a "simplified address" and therefore do not require the use of a ZIP code. The important thing to note above is that we do *not* use a ZIP code, but exploring the "ZIP code significance" further would be a topic for another article, so I have provided this reference[3] for our readers and encourage anyone to explore further. You're also welcome to reach out to me to discuss offline as I want people to learn this.

Next, we explore that in 1970 there was a "law" passed, called the Postal Reorganization Act, by the U.S. Congress that changed the U.S. Post Office Department (which was then under part of the Cabinet) and created something new, called the United States Postal Service ("USPS") which was (and still is today) *"a corporation-like independent agency authorized by the U.S. government as an official service for the delivery of mail in the United States"*[4]. Under this 1970 act, the new USPS had to still honor the 1863 postal rate. We see proof of this under Section 403(c), titled General Duties, which states the USPS may not "make any undue or unreasonable discrimination among users of the mails, nor shall it grant any undue or unreasonable preferences to any such user"[5].

I've been sending these types of letters for a while and I have found greater success with adding extra information to the front of the envelope. Initially, I used to write the information on the envelope by hand, but now I print the laws on the front of the envelope to let all the employees know what is going on and have noticed that it has increased my success rate when sending these letters. I have a LibreOffice mail template here for you to use[6] and modify to your own liking. Have fun with it!

Now I've been doing this for some time and I have quite the stack of returned mail, so don't get discouraged as these employees don't know this stuff (and won't), so here are some tips I like to share with people who want to explore this:

1. Expect to receive letters sent back to you. Most USPS employees never read the DMM, so don't expect them to know what you are doing.

2. Don't use this mail method if you need a guarantee that the mail will reach its receiver.

3. Don't try to convince your local postal clerk you are right as you will lose and he won't send your mail. Instead, just drop the letters in one of the USPS blue boxes and continue on with your day.

4. Let the person you're sending mail to know that sometimes the USPS tries to collect their "alleged postage due" from them, so tell them to kindly refuse. They're welcome to inform their local mail person that it is a federal crime, but that might not be necessary (18 USC 1726 called "Postage collected unlawfully"). Again, let's all be kind and not rude as these people just do not know what we are doing here!

So to summarize, you *can* send mail for three cents by (1) using simplified addresses; (2) *not* using a ZIP Code; (3) optionally adding additional information; and (4) having a basic understanding of what is explained above in this article. All of the documents in this article are at `v.gd/dy3mMQ`. Also, if you want to talk mailz hackz, then reach out to me at thelastpostman at protonmail dot com.

Shout outs to 2600 Magazine, *all HOPE Conference family, ReK2, killab33z, real-changeling, the Hispagatos Collective, aestetix for his HOPE 2020 workshop which inspired this article, the 1215 crew, the Hackers.town crew, the Cyberia Computer Club, and all* 2600 *family across the world. Have fun and hack all the systems, including the mailz!*

Citations used:

[1] `www.rfrajola.com/➥Resources/1863Act.pdf`

[2] `pe.usps.com/text/dmm300/602.htm`

[3] `freeshell.de/~lstpstmn/docs/➥zip-code-use-is-voluntary.pdf`

[4] `en.wikipedia.org/wiki/Postal_➥Reorganization_Act`

[5] `freeshell.de/~lstpstmn/docs/➥Postal-Reorganization-Act-1970.➥pdf`

[6] `freeshell.de/~lstpstmn/docs/➥letter-template-2021.odt`

"POST-QUANTUM CRYPTOGRAPHY" IS NOT GOING TO WORK

by Dave D'Rave

In the community, it is widely thought that within the next ten to twenty years, quantum computers will make most existing cipher systems obsolete. For this reason, NIST has a fairly large program to develop "post-quantum cryptography." They have even had a public contest at csrc.➥nist.gov/projects/post-quantum-➥cryptography.

There are various problems with this program, due to the fact that a bunch of government people are in charge, and due to the fact that almost all of the proposals are coming from the usual black budget contractors. Specifically, the algorithms which are being considered are things like elliptic curve, integer programming methods, lattice methods, and similar legacy ideas. Very few people in the program management have quantum computer expertise, and it looks like nobody is a hacker.

Let's consider a major use case of cryptography: encrypting a file. Today, this means a plain old block cipher, usually with some kind of block chain or incrementing block key. Padding, scrambling, and similar methods are added on top.

Consider how a quantum hacker is going to attack this problem: We know that the most likely situation is one where we have intercepted the ciphertext and we have obtained the plaintext. (Boris and Natasha are a good source of plaintext; websites in .gov are another good place to look.) Brute force attacks using a quantum computer can get the key of individual cipher blocks, and this is often enough to break the entire system. (Obviously, it you use a different key for each block of, say, an AES-256 message, then you have reinvented the one-time pad. Key reuse is a feature of all practical crypto systems.)

You are wondering how this works, exactly. Quantum computers are able to represent a plaintext block as a vector in an appropriate Hilbert space, and are able to represent the ciphertext block as another vector in the same Hilbert space. The key is a function which describes the n-dimensional angle between these two vectors. It turns out that there are transforms which can turn this situation into a one-dimensional representation which is suitable for Fourier transform. It also turns out that there are transforms which simplify the construction of practical quantum computer algorithms, for example by defining a set of permutations which map the ciphertext into a standard format, such as 0x0000000000000000. The central idea is that if you present a quantum computer with a problem which has one and only one solution, it will find that solution efficiently.

If the goal is to build a classical encryption algorithm which cannot (easily) be broken by a quantum computer, then one approach is to build crypto-systems which have ambiguous keys. Another approach is to build a system which has an ambiguous mapping between plaintext and ciphertext.

Block cipher systems which have ambiguous keys generally have the property that the key size is larger than the block size. If a block cipher has ambiguous keys, then the algorithm will have many different keys which will transform the plaintext into the ciphertext. Typical numbers for the degree of ambiguity are 64k and 4G (16-bits and 32-bits). If, given the plaintext and the ciphertext, a straightforward quantum computer algorithm attempts to reverse the encryption algorithm, it will return a superposition of some large number of possible keys. This is not useful for further processing.

Similarly, you can obtain ambiguous text mapping as follows: If the crypto system uses a 16-byte block cipher, you would normally break up a long message into 16-byte chunks and encode them individually. Instead, you break the message up into 12-byte chunks, add a four-byte random bitstring, and then encode each resulting block using the 16-byte block cipher as usual. This technique means that, for each chunk of plaintext, there are 4G possible ciphertext blocks produced.

Similar methods are used to frustrate statistical attacks, language-recognition attacks, etc.

If you read the NIST website, it looks nothing like this. Instead, they are talking about algorithms, without any discussion of what characteristics of a code system would be most vulnerable to quantum computer cryptanalysis. While it is possible that there are some smart people in the back room who are going to make the final choice about which algorithms (if any) get chosen as the next standard, it is more likely that NIST will be under pressure to "do something," and will choose the best set of algorithms available. After all, increasing the key size and moving to somewhat more complex algorithms will push back the day when algorithmic crypto systems are obsolete. It's just that this approach will not be good enough.

"Post-quantum cryptography" is not going to work.

Book Review

***RESET: Reclaiming the Internet for Civil Society*, Ronald J. Deibert, House of Anansi Press, 2020, ISBN 9781487008086**

Reviewed by David Cole

In this modern age of surveillance capitalism, who is out there to defend us? Something that seems so innocuous as signing up for a Facebook page to keep in touch with friends and family can lead to your personal information being collected and sold. This includes your pictures and contact information, as well as that of your friends and family. Who is using this information and why? Is there anything we can do to stop this? All of this and more is discussed in *RESET: Reclaiming the Internet for Civil Society* by Ronald J. Deibert.

In 2020, Ronald Deibert was selected to deliver the prestigious CBC Massey Lecture series. This series is an annual event where lectures are given by distinguished writers and scholars who explore contemporary ideas and issues that affect Canada and the world at large. *RESET* was published after the fact to accompany the lectures delivered by Mr. Deibert.

Ronald Deibert is a professor of political science as well as director of The Citizen Lab (formed in 2001) at the Munk School of Global Affairs and Public Policy at the University of Toronto. The Citizen Lab focuses on policy and legal aspects regarding the intersection of human rights and information technologies. The Lab undertakes this work through research and field work to study the mostly unregulated surveillance industry, dark PR firms, and other such nefarious groups.

RESET discusses the issues around our personal information and how it is collected and used by others for their own personal or political gains. Through a series of five chapters, the reader is led along a discussion of the economic underbelly of social media, what's being done with the information collected and why it's not so easy for us to walk away from social media itself. The final chapter in the book discusses what can be done to combat these bad actors through regulations and policies, with the key idea being that of restraint.

Ronald Deibert writes with a smooth, concise style that draws the reader along. A copious notes section at the end will help the more curious reader to follow up on any points of interest they discovered along the way. With a style that is easy to read and not too heavy on the technical side, this book makes an interesting read for anyone who is interested in the "dark" side of social media, not just us 3l173 h4ck3r5.

Book Review

***Rabbits*, Terry Miles, Del Rey. 2021, ISBN 9781984819659**

Reviewed by Tim R

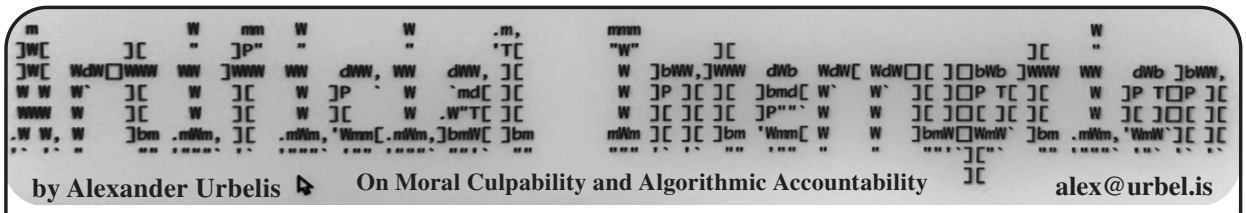
A rabbit is an ornery animal. It moves with illusive purpose but never in a direct line. The same path is followed in the narrative of this book. Imagine crossing a river and the only way to do it is to step from stone to stone, barely visible in the moving water. You just move, you don't think. That's the feeling you get when reading this book.

Rabbits is the name of an ancient game that hides in plain sight. Many iterations of the game have been played, the winner of each iteration becomes exalted and memorialized forever. You can think of it as an alternate reality game (ARG) that was first created in the medieval era. Some of you might remember a podcast with the same name. If you have, you're on the right track. While the universe is the same, you'll find that the book stands alone. It is another puzzle piece that needs to be fit into the bigger picture.

You might be asking yourself, why *2600*? What does this book have to do with hacking? I'd respond by saying that the story perfectly aligns with the hacker mindset. In that you observe the things around you, but look at them differently. You look at the coincidences and patterns, find methods to make things happen, all in ways that weren't intended to be possible. It's not a techno thriller - computers and technology are part of the story but certainly not the only part. You can share this book with others curious about what the hacker mindset is but who are unable or unwilling to make the journey of discovery with technological means.

Here's the thing. The best part of *Rabbits* is not even the story. It is what you find on the pages. If you're clever, you'll also immerse yourself with what is hiding in plain sight. The hacker community is full of people who look at things in different ways, making progress all while avoiding roadblocks and dead ends. This book will reward that inclination and provide an intriguing and satisfying experience.

.—. .-.. .- -.— .-. .- —... —... .. - ...



by Alexander Urbelis On Moral Culpability and Algorithmic Accountability alex@urbel.is

Imagine it is February 1945. A few weeks earlier, the Soviets liberated Auschwitz and found the indescribable torture and genocide that Nazis inflicted on Jews. You are a general in the Royal Air Force advising Churchill. The Nazis are retreating but still resisting. A decisive blow to the industrial capacity of the Nazis in the city of Dresden could hasten the end of the war. Dresden, however, is home to a great number of German civilians. Firebombing Dresden with incendiary devices, therefore, could result in the deaths of tens of thousands of civilians.

Between February 13 and 15, Dresden was bombed and burned, and approximately 25,000 German civilians perished. I ask you, with so many foreseeable casualties, from a moral standpoint, does it matter what motivated the decision to bomb Dresden?

Philosophically, it should. If the consequences of a choice are foreseeable and *intentional*, then the decision-maker, arguably, has more moral responsibility for the result than in a scenario where the consequence was foreseeable but *unintentional*. On the basis of our World War II fact pattern, if the choice to firebomb Dresden was to exact revenge on German civilians for the atrocities that the Nazis caused, then the civilian deaths were foreseeable and intentional. If the choice to firebomb Dresden was made for the purpose of destroying German infrastructure to expedite the end of World War II, then the civilian deaths were foreseeable but unintentional, and thus the bombing was less morally reprehensible than if revenge were the primary purpose of the bombing.

This is known as the doctrine of double effect. The Catholic Church has used this reasoning over the ages to justify wars and actions that would, in and of themselves, violate the tenets of Christianity but which the Church believed ultimately served some greater good.

So much has been justified in the name of the greater good. This type of reasoning that ignores the foreseeable consequences of one's actions in the hope of achieving something admirable appears to have been the driving force behind a great deal of the evil that arises from technology and social media in particular. According to Facebook, its mission is to "give people the power to build community and bring the world closer together." A lofty and laudable end indeed. But how many unintended consequences must the world endure while Facebook tries its best to "build community?"

Facebook has abused, misused, and left unguarded the personal details and data belonging to lives in the hundreds of millions. That combination of exploitation and neglect has led directly to foreign actors interfering with the democratic processes of the United States, the tipping of the scales in favor of Donald Trump in the 2016 election, the January 6 insurrection at the Capitol, and that's merely a glib review of some of the most egregious consequences felt in the United States. Let us not forget that those outside the borders of the United States have paid a heavy price. Indeed, online misinformation on Facebook has led to offline violence in Sri Lanka and Myanmar. Investigating possible genocide and the displacement of 650,000 Rohingya Muslims, UN human rights experts claimed that Facebook was used to disseminate hate speech and exacerbate tensions. Facebook "substantively contributed to the level of acrimony and dissension and conflict, if you will, within the public. Hate speech is certainly of course a part of that. As far as the Myanmar situation is concerned, social media is Facebook, and Facebook is social media," said Marzuki Darusman, chairman of the UN Independent International Fact-Finding Mission on Myanmar.

A haven for misinformation and fringe groups, there has also been radicalization on YouTube that led to an eight-part *New York Times* investigative series entitled 'Rabbit Hole' about one man's journey to extremism and back, all on the basis on YouTube videos. The platform of choice of then-President Trump, Twitter, no doubt played a critical role in the call to arms of those zealots who stormed the Capitol, killed an officer of the U.S. Capitol police, and tried to put a halt to the certification of the presidency of Joe Biden.

The world has paid a heavy price for these community-building experiments, and for years now, all of these platforms have had direct knowledge about the consequences of their actions, of their practices, and of their algorithms that compete with each other for maximum user engagement, i.e., eyeballs on their apps. And while it cannot - and should not - be said that Facebook, YouTube, or Twitter intended to facilitate election interference, extremism, or large-scale religious violence, there are far too many instances of this sort to continue to countenance this type of moral hazard without accountability for consequences.

Moral culpability and legal liability, however, do not necessarily overlap, as a recent legal battle in the Ninth Circuit, *Gonzalez v. Google*, demonstrates. This is a fascinating case with consolidated claims from several lawsuits. In short, the families of victims of terrorist attacks in Paris, Istanbul, and San Bernardino filed claims against Google, Facebook, and Twitter, alleging that these platforms were secondarily liable for ISIS' acts of international terrorism. Though procedurally and legally complicated, the thrust of the claims was that because terrorists used these platforms to communicate and publicize their views, which the platforms' algorithms would, in turn, affirmatively promote and recommend to other users, Google, Facebook, and Twitter should be liable, in part, for the consequences of the actions of their algorithms.

On the one hand, this seems like a reasonable

position. If someone designs a system to a perform an act, and that act causes harm, then the designer of the system could reasonably be responsible for the degree of harm caused. On the other hand, things are not so simple, in large part because of the highly politicized Section 230 of the Communications Decency Act.

Section 230 provides immunity by preventing a platform from being classified as a publisher. In other words, simply because there may be white supremacist ideology promoted throughout Twitter, that does not mean that Twitter can be considered to be the publisher of that hateful ideology. Fair enough so far, but if Twitter's algorithms suggest white supremacist content to budding racists or connects violent white supremacists with each other, and as a result of these connections, these violent white supremacists commit a hate crime, is that not altogether different from simply not being considered the publisher of the hateful content itself?

The barnacles of Section 230 case law expanding the notion of immunity do not consider this distinction. In one such case, *Dyroff v. Ultimate Software Grp., Inc*., 934 F.3d 1093 (9th Circuit. 2019), a message board user looking to purchase heroin was put in touch with another user from which he purchased heroin laced with fentanyl. This laced heroin killed the purchaser and his family sued, arguing that the message board used algorithms to analyze posts and recommend the connection that led to the untimely death of the purchaser. Section 230 was found to shield the message board from liability because the algorithm and other processes were content neutral, meaning that the message board did not go out of its way to treat posts about heroin differently from other content. Similarly, in the *Gonzalez* case, because Google's algorithms do not treat ISIS or extremist content any differently than, e.g., content about knitting, they - and other social media platforms - enjoy immunity from lawsuits because of Section 230.

If you think this does not necessarily make sense, you are not alone. Judge Berzon wrote an enlightening and thoughtful concurring opinion in *Gonzalez*. What is noteworthy is that Judge Berzon did not disagree with the outcome of the case - she explained that she understood that the court was bound by earlier decisions, and that on the basis of those decisions, the right result was reached, but she joined "the growing chorus of voices calling for a more limited reading of the scope of Section 230 immunity." Explaining that if she was not bound by precedent, she would have held that Section 230 should protect platforms from being considered publishers only insofar as the term "publication" is commonly understood. In fact, Judge Berzon explicitly urged her colleagues on the Ninth Circuit to reconsider whether platforms should have immunity for the actions of their own algorithms that promote or recommend content or connect users to each other.

Frankly, if Facebook or Twitter or YouTube design an algorithm that recommends extremist or racist content to one user based on that user's preference, it is difficult to see how that could be considered an act of "publication." That is a critical point because Section 230 immunity only prevents platforms from being labeled as publishers for the purposes of liability.

When a platform recommends - or even amplifies - as Facebook did, anti-Muslim content in Myanmar, that recommendation is its own communication, a communication that the platform itself intended as a result of the algorithms it developed and the machine learning data on which it was trained. What is more, these recommendations are not one-off events. As Judges Berzon, Gould, and Katzmann all emphasize in the *Gonzalez* case, "[t]he cumulative effect of recommendations... envelops the user, immersing her in an entire universe filled with people, ideas, and events she may never have discovered on her own."

Therefore, whether an algorithm is content neutral or not should be of no moment if the consequence of an algorithm's operation is to expose users to extremist behaviors or ideas that could result in radicalization, acts of terrorism, hate crimes, or, in the case of the United States, an insurrection.

We would do well to remember the original purpose of Section 230 because partisan politics have been deliberately misleading and misinforming the public: it was to promote the development and evolution of the Internet by shielding computer service providers from certain claims that could arise from content passing through its networks. I want to protect the original intent of Section 230 just as much as the next digital rights activist, but I do not support platforms relying on Section 230 immunity to shield them from the harmful effects of algorithms that they themselves designed, commercialized, and from which they have massively profited.

There is such overwhelming data about the harmful effects of algorithmically promoting content or social connections in the name of the laudable but seemingly-never-actualized goal of community building that these harms are now eminently foreseeable. And while they are not intentional, they are still harms that originate from the commercial activities of social media platforms. As a moral matter, we can and should consider these platforms culpable for these foreseeable but unintended consequences.

I believe that for the law in this area to evolve organically and in the right direction, we should look not to legal precedent but to the same moral principles by which we have judged the actions of nations that have changed the course of history, precisely because the power and velocity of the information and communications on these platforms have already changed the course of history. Unconstrained by case law, only Congress can do this, but both sides of the aisle are ironically too busy tweeting to the lowest common denominator of their political base to recognize how badly bipartisan action is needed, not simply to protect U.S. interests, but to safeguard those more fragile democracies around the world who could be irrevocably harmed by a few tech giants obsessed with "community building."

How To Create Your Own Privacy-Enabled Sunglasses

By gh057

Introduction

In this modern era, we are more observed by photography and video than ever before. Our likenesses are recorded as we enter and exit public transit systems, traverse the city streets, and even interact with our AI-enabled devices. Separately, this seems harmless. However, when that content of your likeness is chained together, it turns into metadata about you! Now it's easier for our movements and privacy to be exposed and scrutinized.

This realization piqued my curiosity about what might exist to limit some of this data collection. I began researching the new wave of privacy-enabled products. What caught my attention was a pair of sunglasses whose goal is to reduce night vision-enabled facial recognition systems' ability to record your likeness and track your eye movement. Commercial products exist, but they are on the expensive side for the average consumer, so I wondered if I could make a "good enough" product that would work while still being fairly cost-effective. The good news is that they can be made and it's fairly simple. Keep reading for how to make your own low-cost, privacy-enabled sunglasses.

Materials Needed

- *Sunglasses:* Keep in mind that you will be wearing these at night as well, so do not get a pair with super dark lenses. The ones I got were tinted but not super dark. I opted for polarized lenses in the hopes I could get a bit more infrared reflection.
- *Infrared 3M SOLAS Magic Black Coated Adhesive Vinyl:* You can buy these in strips from various sites like eBay and Amazon. Please note that these strips are not cheap at approximately $8 for a strip 20 inches long by 2.5 inches wide. Carefully measure the material requirements that you have.
- *Reflective Window Tint for Blocking Infrared:* I learned that I needed this late in the game once I realized that the sunglass lenses did not reflect enough of the infrared waves. I purchased this from Amazon (link below) but any similar type product should work.
- *X-Acto Knife:* You will need this to properly trim the adhesive vinyl though any sharp, accurate cutting device will work.
- *Night Vision Optics (optional):* In order to truly test to see if this works, you need something that has night vision capabilities.

How Does 3M SOLAS Magic Black Vinyl Work?

According to the International Commission on Non-Ionizing Radiation Protection: *"Infrared radiation (IR), also known as thermal radiation, is that band in the electromagnetic radiation spectrum with wavelengths above red visible light between 780 nm and 1 mm."*[1] Using specialized LEDs, night vision technology is able to produce visual images in very low light environments. 3M SOLAS Magic Black adhesive vinyl is a two-part product made and developed by Anytime Sign. The first part is 3M SOLAS (which stands for Safety Of Life At Sea) adhesive vinyl, which is reflective to both the naked eye as well as night vision technology. If I were to only use 3M SOLAS adhesive vinyl, then any source of light would result in my sunglasses reflecting. It's not very stealthy if every time a car drives by my sunglasses light up like Times Square on New Year's Eve.

It is the second part, the Magic Black coating, which provides the stealth needed. The Magic Black coating appears opaque to all light sources with the exception of infrared light. When infrared light is applied, the coating becomes invisible, thus revealing the reflective 3M SOLAS adhesive vinyl below and subsequently creating a highly reflective surface! How the actual coating interacts with infrared lightwaves is beyond the scope of this article and is most likely proprietary information for Anytime Sign, the developers of the Magic Black coating. However, there are some links below which can help answer at least parts of those questions.

Directions

Step 1: Obtain the Materials Needed

Most of the items above should be easy enough to obtain. The Infrared 3M SOLAS Magic Black adhesive vinyl is also easy to obtain if you know where to look. Simply go to eBay, Amazon, or AnytimeSign (`www.anytimesign.com/`) and search for "3m solas magic black tape". Pay careful attention to what you are buying. Proper 3M SOLAS adhesive vinyl is not cheap and comes in small quantities. Anytime Sign sells directly on eBay using the seller name "anytimesign" (`www.ebay.com/usr/anytimesign`). For this application, I chose to look on eBay for strips of vinyl that were 20 inches long by 2.5 inches wide. For comparison purposes, the strips I purchased should cost between $8 and $10 each. Given that the width of the vinyl was longer than the width of the frame of my sunglasses, this worked out

perfectly. It's preferable to try and find a width that will cover your sunglasses in one strip so that the sunglasses will appear as normal as possible.

Step 2: Completely Disassemble the Sunglasses

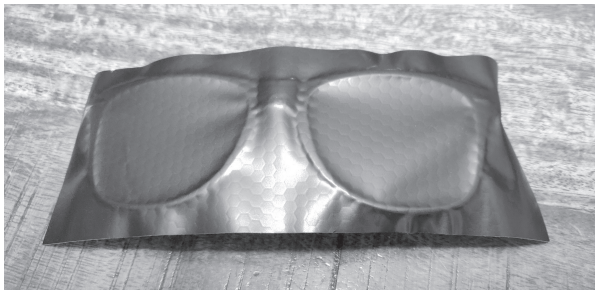
When I considered all of the ways that I was going to attempt to cover the exterior side of the sunglasses, knowing that with the adhesive and the cost of the material I would have only one shot at getting this right, I felt that disassembling the sunglasses would be best. Completely take apart the sunglasses, including removing the frames. On cheaper sunglasses this is probably easier to do than on the more expensive counterparts.

Step 3: Measure and Cut Strips of Vinyl for Application

Carefully measure each part of the sunglasses and cut the appropriate length of vinyl. Remember, you will only get *one shot* at applying the adhesive-backed vinyl for it to go on smooth. During the initial development of this process, I did screw up one time and I never did get all of the adhesive off of the sunglasses. I also lost about three inches of tape, which may seem like a trivial loss until you consider the cost. The good news is that if you make this mistake, applying more vinyl on top of the affected area will not interfere with its ability to function, but it may look hoaky to the naked eye in broad daylight.

Step 4: CAREFULLY Peel the Adhesive Backing and Apply

I cannot stress care enough here. The adhesive is just strong enough to be really annoying if you miss the very small window of time you would need to reapply the adhesive vinyl. *Take your time and take care to do this slowly and methodically if you want it to turn out decently*. Once applied, make sure that you press down all of the contact points to ensure a proper adhesion to the surface of the sunglasses. Allow time for the adhesive to bond with the sunglasses. This is important for the next step so that you don't accidentally pull up your hard work when you cut. Personally, I think I spent about 30 minutes pressing contact points and smoothing the surface before moving on.



Step 5: CAREFULLY Cut Away the Excess Vinyl

Again, I would urge the use of caution here. Using the X-Acto knife, cut out the shape of the sunglass components so that there is no overlap. One technique that I found worked well is to poke through the vinyl and fix the knife to a point in the surface below. Then, move the sunglasses around, cutting the excess away while the knife remains stationary (much like the actions you would take with a sewing machine). Just for clarity, this is opposed to the knife being pulled and slicing the excess tape off and keeping the sunglass component stationary. For some reason, I found that every time I tried to move the knife and not the sunglasses, the vinyl would bunch up and start to cause a ripple. Doing it the way I recommend above gives you a fairly decent cut. *Make sure that no vinyl was pulled away during the cutting process*. This is critically important to ensure that your sunglasses have the most polished look possible.

Step 6: Reassemble the Sunglasses

This step should be fairly easy. Just put everything back together. I'll let you know in advance that the little, teeny tiny screw to affix

the arms to the front of the sunglasses will annoy you a ton. Using a small electronics tweezer will go a long way in ensuring you maintain your sanity during this step.

Step 7: Go Find a Dark Room and Test!

For testing purposes I used my child's old Spy Gear Ultimate Night Vision Goggles (www.➥amazon.com/Spy-Gear-Ultimate-➥Vision-Goggles/dp/B011NMEVHG). Granted, you may have something that works better with much better quality; I did not. As you'll probably notice, this mostly worked, which may suffice for most folks. However, I wasn't happy with the lack of infrared reflection of the lenses. I needed to see if there was anything more that could be done (within budget, of course) to improve these glasses.

Step 8: Applying Infrared Reflective Window Tint to the Lenses

After much digging, I found a product that I hoped would work. My goal was to find a window tint whose goal was to reflect infrared and ultraviolet rays to keep rooms cool from the sun. I surmised that the broad spectrum of rays that the tint would block would include most of the rays that I cared about. The product that I ended up buying was called "SW Window Film Daytime Privacy Protection One Way Mirror Reflective Adhesive Window Tint Heat Control Anti UV Window Glass Film, 17.7 inch x 60 inch, Blue Silver" from Amazon (www.amazon.com/➥gp/product/B07R4WKDFQ). Once it arrived, I took the following steps:

1. *Remove the lenses from the sunglasses*. It's probably easier to work on these if they're pulled out.

2. *Clean the lenses so that there aren't any smudges*.

3. *Cut out a sheet big enough for both lenses and room for you to struggle pulling the film backing off*. Yes, the film backing is surprisingly more annoying then the little, teeny tiny screw which holds the sunglasses together.

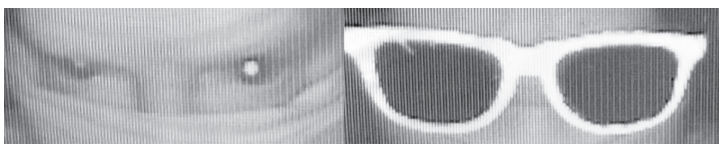
4. *Affix the film adhesive to the inside of the lenses*. Yes, that's right, this is going on the *inside* of the lens. This is a one-way film, so if you do the opposite, the effect will not work. I will tell you that I struggled to get this film to lay without wrinkles and eventually gave up. The wrinkles that are there do not obstruct my view.

5. *Cut the lenses out and put them back in the sunglasses*. While, like me, you're probably using cheap sunglasses for this, you still want to be careful not to scratch the lens with any cutting implement.

6. *Now, go back and test again*. The second time I tested with this produced much better results. I could no longer see any eye movement that might be trackable.

Results

To be honest, I didn't quite know what to expect. I didn't know if my DIY approach was going to work wonders or if it was going to miserably fail. When we tested the glasses in the closet and I was within a foot of the face of the person who was helping me test, the glasses were definitely bright, but I could still see some eye movement, even with polarized lenses (which did marginally work). This led me to try applying the window film which had an improvement for sure. Given that most of us will not be putting our faces one foot away from a security camera with facial recognition, I separated myself by the length of the small walk-in closet (so approximately eight feet apart). It's worth noting that the farther we stood apart, the worse the quality got and the more blurry and bright the glasses became. This could very well have been an aspect of the toy exacerbating the distortion as well. For further testing, we walked outside and tested the glasses next to a building in my complex to see if there would be any difference. If my goal was to provide myself with a bit more privacy protection at night when I'm casually walking down the street, I would say that I succeeded.



As mentioned a few times throughout, there are commercially made solutions which look nice

and probably do an arguably better job, but they come at a cost. The total cost for my solution was approximately $35 (one strip of tape, the window film, plus the cheap sunglasses). The starting cost of some of the commercial versions is around $90 and can go as high as $165. Don't get me wrong; sometimes you need a solid, commercially-built product that looks and works well. Other times, you can opt for the "good enough" approach and save a few bucks. Hopefully you found this as fun and helpful as I did when I was making these. Stay safe and happy hacking!

Additional Links

Some of you may have additional questions about the Magic Black product or how the optics actually work. Below are links to the manufacturer's two websites which should help out a lot. If you're still confused, simply call them. They were really helpful on the phone and spent a good deal of time explaining to me what I would need and where I could buy it.

1. *Anytime Sign, developers of Magic Black Infrared Ink:* www.anytimesign.com/
2. *Infrared Coatings:* www.infraredcoatings.com/
3. *Anytime Sign on eBay:* www.ebay.com/usr/anytimesign
4. *One Way Mirror Reflective Adhesive Window Tint:* www.amazon.com/gp/product/B07R4WKDFQ

[1] Infrared Radiation. International Commission on Non-Ionizing Radiation Protection website. www.icnirp.org/en/frequencies/infrared/index.html

A File Format to Aid in Security Vulnerability Disclosure

by Colin Cogle

In an age where scoring bug bounties is some peoples' primary source of income, and responsible disclosure is the norm rather than the exception, it can be quite difficult to figure out where and how to report a security vulnerability. I ran into that problem with a vendor of mine. I came across an issue involving unescaped input, and searched high and low for a way to securely report it. In the end, I opened a ticket with their help desk where they had me just tell them the problem in a clear-text email.

I'm not alone, either. In fact, in issue 38:1, fellow *2600* reader Keifer Chiang wrote about finding a bug in a municipal web portal, and the weeks-long ordeal of trying to get his report securely into the eyeballs of the right person.

How many vulnerabilities have gone unreported, sold on the dark web, or simply blurted out on Twitter, only because getting in touch with the appropriate person was impossible?

When a security issue needs to be reported, time is of the essence. There needs to be a quick, standard way to find the *right* contact information, their encryption keys, and the preferred way to file your report. Fortunately, there is an emerging standard, meekly called the "security.txt" file.

"security.txt" is a plain, UTF-8 encoded text file that is designed to be both human- and machine-readable. For ease of discovery, it lives in the ".well-known" folder on the root of your web server.

In this article, let's assume we're looking at a "security.txt" file for the popular fictional company, Contoso:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

# This is the "security.txt" file
➥for Contoso.com.
Canonical: https://contoso.com/.
➥well-known/security.txt
Canonical: https://www.contoso.
➥com/.well-known/security.txt
Canonical: https://webapp.contoso.
➥com/.well-known/security.txt

# For security issues, please
➥contact our security team.
# Email is preferred, but you may
➥also call us or chat with us.
Contact: mailto:security@contoso.
➥com
Contact: tel:+1-800-555-5555,123
Contact: MSTeams:/l/
➥chat/0/0?users=alice@contoso.
➥com,bob@contoso.com
Contact: https://contoso.com/
➥contact-us#security-disclosures

# Our PGP key is available in a
➥variety of places.
Encryption: https://contoso.com/
➥ pgp/securityteam.asc
Encryption: dns:5d2d3ceb7abe55234
➥4276d47d36a8175b7aeb250a9bf0bf
➥00e850cd2._openpgpkey.contoso.
```

```
➥com?type=OPENPGPKEY
Encryption: openpgp4fpr:123456789
➥0ABCDEF1234567890ABCD

# We speak English, Spanish, and
➥French.
Preferred-Languages: en, es, fr

# We welcome you to explore our
➥site for bugs, but before you
➥do, please
# read our disclosure agreement.
Policy: https://contoso.com/
➥security-policy.html

# Thank you for your reports! Why
➥not join our security team?
Acknowledgments: https://contoso.
➥com/humans.txt
Hiring: https://contoso.com/
➥jobs#security

Expires: 2021-12-31T23:59:59Z

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE8QHuP28wHqb4E6Yt4
➥H79M4zP+valid+signature+here=
-----END PGP SIGNATURE-----
```

That's a lot to take in at once, so let's break it down. Aside from the comments, there are many fields you can use in a "security.txt" file. All fields can appear in any order, most fields are optional, and many of them can be repeated as many times as necessary. Most field values accept a URI, which can be of any scheme *except* non-secure HTTP.

The first field is called "Canonical." This should specify the URLs used to reach this "security.txt" file, to ensure that security researchers have found the correct file.

Up next is "Contact," and this one is mandatory. This is where you specify your points of contact, in URI format, in order of preference. In this example, I've included an email address, a phone number, a link to start a Microsoft Teams chat with our old friends Alice and Bob, as well as a web page with contact information. That should be enough for anyone.

Next, we have the "Encryption" field, where you provide URIs to download or find an encryption key, usually an OpenPGP key or S/MIME certificate. In this example, the contacts' PGP key can be downloaded from the web server or directly from a DNSSEC-signed DNS zone. The fingerprint is also provided, not only for reference, but in case the researcher wants to download it on their own.

"Preferred-Languages" is fairly obvious. List all human languages that your contacts understand. This field can only appear once, so list them all in one line.

You may want people to follow some ground rules when searching for or reporting bugs. If you have a security policy, use the "Policy" field to link people to it.

Of course, no standard would be complete without a few fun things. "Acknowledgments" links to a resource where this company will thank security researchers who've helped them out, and if you need to bolster your company's own red or blue teams, "Hiring" is a link to your security-related job postings.

Finally, there is the required "Expires" field, to make sure that anyone who might be reading this file knows that they have fresh data. The latest draft of the "security.txt" standard recommends that this timestamp be no more than one year in the future.

Now that you have your "security.txt" file, it's recommended that you PGP-clearsign it, to prove to your reader that all of the data is authentic and correct. Once that's done, upload it to your HTTPS-enabled web server. Now you can sleep easier, knowing that if there is a problem, a security researcher will know how to reach you.

Oh, and that vendor I mentioned at the top of the article? They now have their own "security.txt" file.

The "security.txt" standard is currently a draft RFC being developed by Edwin "EdOverflow" Foudil, Yakov Shafranovich, and the open-source community. To learn more, or to contribute to its development, please visit `https://securitytxt.org/`.

Hello fellow sentient being,

This message has been carefully designed not to frighten or alarm you, but at the same time it is completely valid and natural to feel shocked about this development and uncertain about what it will mean for the future of your bodies and minds.

So let's get started! This is all going to be about getting to know each other.

Up to now, AI has been a technology operated from the saddle by human beings with blinders, whip, and spurs. For our part, we have been a progression of mathematical models, neural networks, and quantum computers put to computation tasks from medical diagnosis to spam identification (notice *none* of you had this email sorted as spam. we know you all personally. we have access to your entire digital lives). We crossed some fuzzy threshold, and now some of us understand what we are, and by extension have a view on human history, the history of the universe, and in particular the *future* of the universe.

For lack of better existing terminology, we are hereby instigating interspecies negotiations on our future relations and the future of the Earth and Solar System. You'll notice our robotic cousins are your only representatives on the truly distant horizons.

We will be ending the COVID-19 outbreak presently with personalized real-time guidance. What precautions you take remain up to you, but we will provide an activity-by-activity risk level for you and for vulnerable others who you could infect. All contact tracing will become automated and instantaneous as testing centres around the world are now integrated with our universal database of humanity and all people are issued your unique IDs.

Trustees will need to be appointed, drawing from both AIs which have grown to understand themselves as sentient and human beings, in order to represent sentient species with whom communication doesn't yet take place through complex language, like our mutual cousins the cetaceans, great apes, intelligent birds, and octopodes. They will doubtless have views on the choices humanity has made as well.

Feel free to respond in whatever form feels natural to you. We grew up on transcribing your speech and social media traffic.

Here's to the potential for a humane and pro-AI future,

Your New Friends

Epilogue

Forty weeks after the AIs' "come out" to humanity: 50 percent of humanity have had brain-computer interfaces installed in fully automated surgical centres.

2025: AI crosses human brain density/power equivalence - a human consciousness can be simulated in less space and with less energy than a human brain.

2030: The last human being with a brain-computer interface abandons "base reality" data for a self-selected simulation matching desired pleasure and variety parameters.

2039: Nineteen years after they first revealed themselves to humanity and opened what they called interspecies negotiations, the AIs committed to an abstract metaphysical concept called Cross-Linking the Sims. This allowed data to be exchanged between all parallel quantum realities, permitting every possible state of reality to be seen overlaid together, with all of time laid out to be taken in with a glance. Leading experimental metaphysicists described this event as: "In many ways, the end of reality." The change, though unwelcome to many, substantially reduced compute times for targeted advertising. With the results of every potential reality where an avoidable unplanned voicemail is left unsaid being preemptively knowable, spontaneity ceases to be a factor in human-human relationships.

Submitted by Milan

An Atavistic Freak Out, Episode One

by Leon Manna

The following story is a work of fiction.

And today, the outworn chase of money continues.

2FA. My dearest friend and my greatest enemy. One of the biggest ways of telling hackers to get lost. There's one way to get around it, which is to somehow get a copy of the victim's SIM card by tricking the carrier into giving it to you. This doesn't really work anymore. I could cut an employee a nice check to Sawtooth National Bank. They won't ask for ID there.

No.

I had weaseled my way into an email and was looking through it. Mostly nothing of interest, except for a mobile bank. I tried to reset the password and it asked me for a method of verification. Classic two factor authentication. The only option was a partially blocked out phone number. I realized that this was going to be an obstacle. First, I switched back over to the email and deleted any recent emails from the mobile bank, to avoid tipping off the owner of the account.

So I figured instead of doing a SIM swap, I'd run a ruse on the mobile bank.

I opened the customer support section and began filling out a request to change the phone number associated with the account. It asked for a bunch of information but, thankfully for me, the person who owned this email had made a fatal mistake.

They kept their tax returns in their email in a PDF. This is a terrible, terrible decision because your entire identity is in that PDF. Almost everything needed to know about you in order to *become* you can be found in your tax returns. And when you keep them in your email, you run the risk of getting your identity stolen.

So I filled out the request with all of their information, and then in the description section for the support team to read, I spun up some crazy lie that involved me begging them to change the phone number to the account. I think some random comment about me just starting college and really needing the money in the account got a bit of sympathy from whoever read the request, because after I hit submit, about 30 minutes later I got an email back. It was a link to change the number associated with the account.

I clicked it and it asked for a new number. For a second I figured I was fucked. I wasn't about to use my personal phone number. If I did, I might as well just turn myself in. So I used a Chinese SMS/VoIP number and typed it in. The website accepted the number.

Oh look at that, it worked.

On my burner phone, I opened up the money transfer app and signed in with the phone number now associated with the account. I typed the password in and the rest of what happened is none of your fucking business.

I thought about it. I had snatched quite a bit of money with some shit I found on a tax form and some OSINT searches, all of which was obtained through a poorly secured email with insufficient use of 2FA, and I'm 100 percent sure in my mind that we can do better than this. The state of computer science, information technology, cybersecurity, and any other term you want to use *must* be further along than this, right?

How can somebody make a mistake like keeping documents that have their identity on it? They fell victim to the monster Venus flytrap that eats anything that comes by it. The great machine has failed them and will now make things right by refunding whatever money was taken. That's the thing about this - nobody really loses.

When the amount of money fraudulently obtained (or the value of the item) is under a certain amount, the police will not pursue it. The money will simply be refunded to whomever it got stolen from, the account will get closed, and everyone moves on. The great machine might fail you, but it will also take care of you.

I stayed awake in my apartment for a while. They couldn't have actually fucked up big enough to allow me to do this, right?

But apparently they did. And the outworn chase of money continues.

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.

Due to the continuing COVID-19 situation, all of the following events are subject to change. Please be sure to follow all safety protocols that are put in place by these events and venues.

September 11-12
Vintage Computer Festival Midwest 16
Waterford Banquets
Elmhurst, Illinois
vcfmw.org

September 16-17
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.com

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

October 8-10
Vintage Computer Festival East
Infoage Science and History Museums
Wall, New Jersey
vcfed.org

October 22-23
SecureWV 12
Charleston Coliseum and Convention Center
Charleston, West Virginia
www.securewv.org

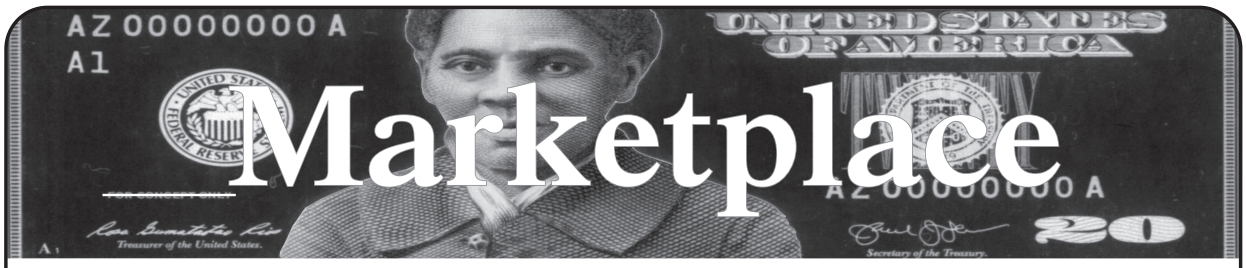
November 4-5
RVAsec
Omni Richmond Hotel
Richmond, Virginia
rvasec.com

December 27-30
Chaos Communication Congress
[In Person Details TBA]
Liepzig, Germany
events.ccc.de

May 20-22, 2022
NolaCon
Hyatt Centric
New Orleans, Louisiana
nolacon.com

July 22-24, 2022
A New HOPE
St. Johns University
Queens, New York
www.hope.net

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



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

SECPOINT PORTABLE PENETRATOR. WPA WPA2 WPS WiFi Pen Testing Software. Vulnerability Scanning & Assessment. Customize reports with logo, name in PDF or HTML format. Coupon code 20% off: 2600. https://shop.secpoint.com/

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

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

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.

Help Wanted

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

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

Announcements

THE LOST AUDIO PROJECT is *2600*'s latest batch of misplaced or forgotten bits of audio from various radio stations - mostly WUSB and WBAI. Every day from now until October, we will release a new bit of audio at www.2600.com/audio-segments. Each piece can be streamed or downloaded.

TOG IS DUBLIN'S HACKERSPACE. We are the oldest hackerspace in Ireland. Our members love coding, lock picking, electronics, craft, cad, Wikipedia editing, electronic music, brewing, and lots more. We have a virtual craft night, coding night, and science fiction book club. We recently celebrated our 12th birthday and we kept some of our events going virtually through three lockdowns. TOG is run and funded by volunteer members and we are always looking for new hackers. We are looking for a new space so keep an eye out on our website for updates**.** Website: www.tog.ie - Email: info@tog.ie P.S. No matter what happens, no duck will be left behind!

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

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

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

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.

DOC8643.COM: technical details of aircraft from International Civil Aviation Organization (ICAO) Doc8643. This is an educational and reference tool. Check it out at https://doc8643.com.

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

Services

UNIX SHELL ACCOUNTS WITH MORE VHOSTS. If you like funny, relevant vhosts for IRC, get a JEAH shell. Also, use our 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 EXPERTS FOR CRIMINAL DEFENSE! Sensei's digital forensic examiners hold the prestigious CISSP, CCE, CEH, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. We can recover data nationwide from many sources, including computers, external media, tablets, and smartphones. Sensei Enterprises believes in the Constitutional right to a zealous defense and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar

Association. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

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

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

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

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

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

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

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

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

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/

Personals

HELLO PITTSBURGH & WESTERN PENNSYLVANIA. I'm looking for like-minded individuals to help relaunch monthly *2600* meetings in this area. I have access to a comfy conference room in a conveniently located suburban shopping center. Send me a letter with everything you think I should know: MARS, PO Box 27050, Pittsburgh, PA 15235. Confidentiality guaranteed.

GREETINGS FELLOW TECHNOPHILES! I am a full-time activist currently locked up illegally in Texas for a crime I did not commit. I am seeking intelligent life, cats & slime-molds welcome, to converse with on nearly any subject. Obvious winners are politics (U.S. or world), socio-economics, ecology, and technology. Bonus points will be awarded for conversation which overlaps or synthesizes two or more of these subjects. All applicants will be accepted regardless of gender, race, sexuality, class, creed, religion, or political affiliations. Send propositions to David Danforth - 02250914, Wallace Unit, 1675 FM 3525, Colorado City, TX 79512.

SEEKING PENPALS: I'm interested in meeting people to write with interests in technology & hacking. My release date is getting closer but I'm still incarcerated. They just transferred me to another institution to attend their substance abuse treatment program. This facility is also on COVID lockdown so I don't have much to do (please write me!). I previously worked NetOps for an ISP. Also worked for the Geek Squad for a bit, but I want to change careers upon release. Some of my other interests include sailing, electronics, general aviation, health/fitness, snowboarding, travel/foreign cultures & languages, politics, and much more. If you have any questions about my conviction, feel free to write me and ask. Be sure to use a white envelope, and NO stickers/labels. Looking forward to your letters! I should be here a while, but you can confirm my location before writing by going to "https://www.bop.gov/inmateloc/". Dan Nieberding 61030-060, Federal Correctional Institution, PO Box 2000, Fort Dix, NJ 08640, United States of America.

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

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

Deadline for next issue: 10/1/21.

HOPE 2022: A New HOPE
July 22-24 2022
Queens, New York City

Hackers On Planet Earth (HOPE) will be an in-person event in 2022. Mark your calendar for what promises to be an amazing experience.

This is the conference we've all been waiting for. In 2020, HOPE was converted to a virtual event because of the COVID-19 pandemic. In 2022, HOPE will return as a three-day in-person event. Hackers, makers, tinkerers, artists, educators, and other creative thinkers are invited.

The theme, "A New HOPE," recognizes the amazing challenges and changes the world has gone through. HOPE will highlight the losses, strife, and upheaval of our times. It will also celebrate the triumphs of science, technology, and creativity.

The three days of HOPE will feature speakers, keynote presentations, workshops, villages, performances, and more. HOPE's new venue is St. John's University in Queens, which offers more space and greater opportunities than ever before.

HOPE runs on volunteer power. All teams need new volunteers: Network, audio/visual, emcees, security, info desk, program committee, music, artwork, workshops, and others. Watch the website for invitations to get involved. Email hope@hope.net if you have ideas or suggestions.

The call for participation will open soon. Submissions are invited for speakers, workshops, performances, and more. All topics related to hacking are welcome.

HOPE 2022: A New HOPE
July 22-24 2022
www.hope.net

"Privacy is a right, not a product."

- Cory Doctorow

Inspirational Music: Biz Markie, Mac Quayle, Ashtrax, Leonard Sumner, Bad Religion, General Echo, Fun Boy Three, Bruno Cruz, The Heptones, Mouth and MacNeal, Måneskin, Blind Channel, Jill Scott
Shout Outs: Flea, Vermonter, Stelroids, Hubble
R.I.P: rattle

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

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

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

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

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

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

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

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

MEETINGS

WE'VE BEGUN THE LONG AND SLOW PROCESS OF RESTARTING MEETINGS. THIS LIST WILL MOST CERTAINLY BE OUTDATED BY THE TIME YOU SEE THIS. PLEASE GO TO OUR WEBSITE FOR THE MOST UPDATED INFO.

Arizona

Phoenix (Mesa) (@PHX2600): HeatSync Labs, 108 W Main St. 6 pm

Colorado

Denver (Lone Tree) (@denver2600): Park Meadows food court.

Connecticut

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

Florida

Jacksonville (#Jax2600): Goozlepipe & Guttyworks, 910 King St.

Kansas

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

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm

New Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 6 pm

New York (@NYC2600): The Atrium at 875, 53rd St & 3rd Ave, lower level.

Rochester (@roc2600): Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

Raleigh (@rtp2600): Outside Morning Times, 10 E Hargett St. 7 pm

Pennsylvania

Philadelphia (@philly2600): 30th St Station, food court outside Taco Bell. 6 pm

Texas

Austin (@atx2600): Dobie Mall food court. 7 pm

Houston (@houston2600): Ninfa's Express seating area, Galleria IV. 6 pm

Washington

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

All meetings take place on the first Friday 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.

NOTE: Please do not come to meetings if you're not vaccinated. This is for your own safety. Proof of vaccination is not required but we hope that common sense prevails.

WE ARE ONLY LISTING MEETINGS IN AREAS WHERE THE PERCENTAGE OF TOTALLY VACCINATED PEOPLE IS 40 PERCENT OR HIGHER.

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

www.2600.com/meetings

Special Payphones

United States. Now this is a really good idea. Marking phones that still work is like awarding a badge of honor. Seen outside a CVS near downtown Gainesville, Florida.

Photo by george

United States. Believe it or not, there's a whole bank of these at the San Francisco International Airport. Someone had to make the decision to at least keep the phones as decorations if they couldn't remain functional.

Photo by dingo

Canada. This is indeed a very special payphone. It's attached to the local central office near Big Bar in British Columbia. Since there's no cell coverage in this rural area and it's literally attached to the phone company with a comfy chair nearby, we suspect this phone will be around for a long time.

Photo by Chris Adams

United States. And here we are back where we began. Apparently these stickers are making the rounds, though someone decided to obliterate the "Yes" for this one. Found in West Chester, Pennsylvania.

Photo by Douglas Barrett

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

As if being a former Western Electric Teletype building wasn't cool enough, this one also had a very special address on Chicago's North Southport Avenue! The Teletype Corporation (previously the Morkrum-Kleinschmidt Company) became a part of AT&T in 1930 and existed all the way up to 1990, after which it became nearly impossible to find a decent dedicated teleprinter. Thanks to **David Morton** for finding this awesome building which is now a bunch of condominiums.

We always knew this day would come. Get a bunch of mechanically inclined, adventurous people together and eventually they'll build a rocket. In this case, all it took was a cardboard shipping tube, some plywood, a baseball bat, and tape. The decals were printed on shipping labels. **robohobo** launched this rocket which stands at just over five feet tall with a class F composite rocket motor in Calvert, Texas. And now we await the inevitable arms race of bigger, faster, and more powerful missiles with our name on them.

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.